Magic Quadrant for IT Event Correlation and Analysis

Gartner RAS Core Research Note G00208774, David Williams, Debra Curtis, 13 December 2010, RV3A412152011

This Magic Quadrant addresses mature and emerging products that help IT organizations consolidate, analyze and respond to component-level IT infrastructure events, improve event-to-incident/problem resolution processes, and improve alignment between events and business-oriented IT services.

WHAT YOU NEED TO KNOW

Gartner's Magic Quadrant for IT Event Correlation and Analysis evaluates vendors' Ability to Execute and their Completeness of Vision relative to a defined set of evaluation criteria regarding current and future market requirements. A Magic Quadrant should not be the only criterion for selecting a vendor, because the right solution for a given situation can be in any quadrant, depending on an enterprise's specific needs. Enterprises considering the purchase of an event correlation and analysis (ECA) product should develop their own list of evaluation criteria and functional requirements in the categories of event collection/consolidation, processing/correlation and presentation.

Large enterprises should consider a multitier event management hierarchy, pushing some event processing and correlation out to the managed IT element at the bottom of the hierarchy. These enterprises should use specialized event management tools in the middle, and should place a manager of managers (MoM) or a business service management (BSM) product on top.

When investing in event management, prospects should understand how the product will fit with their overall event-to-incident/problem resolution processes, including workflow, escalation and integration with service desk tools.

MAGIC QUADRANT

Market Overview

ECA products help IT operations personnel contend with the deluge of events that comes in from the IT infrastructure by eliminating duplicate event signals, filtering events according to operational or business priorities, and analyzing events to determine their root causes. The goals are to improve the mean time to isolate and repair problems, and to prioritize IT support efforts according to business process value.

The core value proposition of these products is to achieve management by exception. This requires an understanding of "normal" behavior in the IT infrastructure and alerting the IT operations staff only when an exception occurs, such as a failure or a threshold breach, indicating that the IT infrastructure is no longer behaving "normally." With the 2010 Magic Quadrant, the desire to associate events with potential business impact has transitioned from a "wish list" item to something that's required for current product execution, although not all ECA vendors offer this functionality.

Gartner

IT organizations invest in ECA tools to improve the productivity of the IT operations staff by reducing the time it takes to troubleshoot problems by consolidating events from various devices, applications and other management tools. Without proper event management, the IT operations group can be deluged with event storms, false positives, a "sea of red" on their console and an inability to reduce the impact an IT event has on the business.

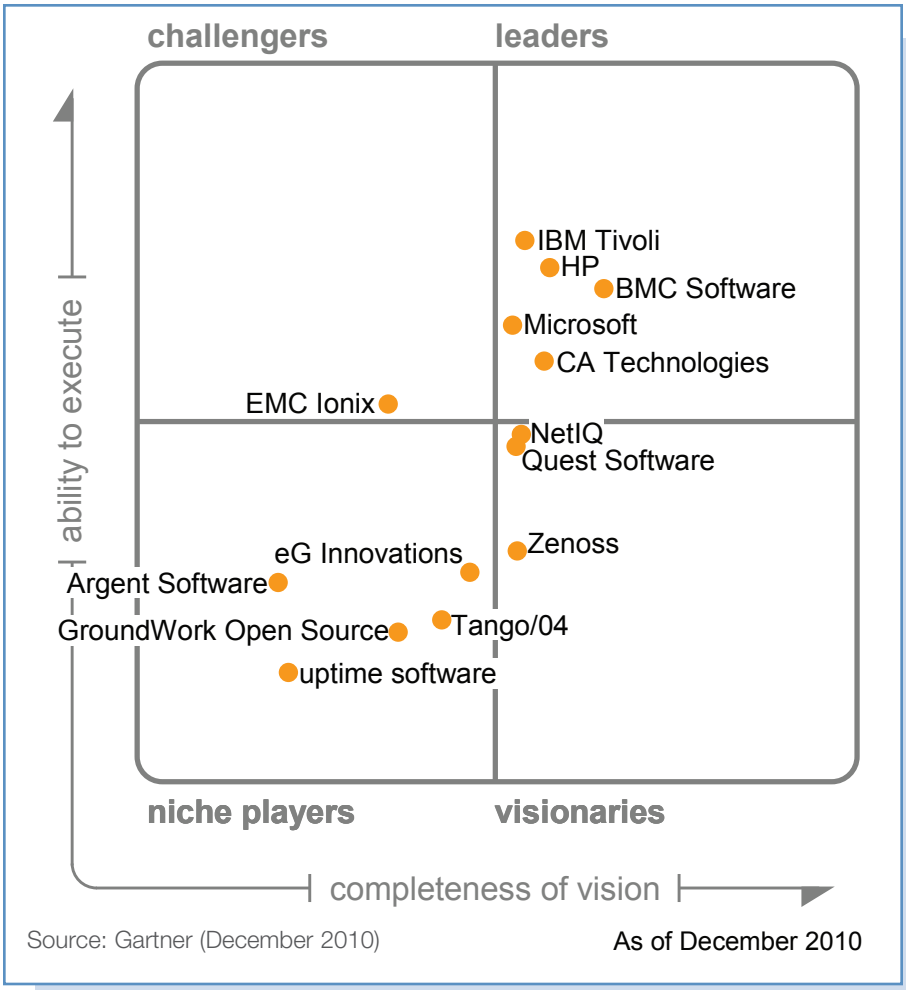
How to Use This Magic Quadrant to Assist in Vendor Selection

The vendor positions on this Magic Quadrant are based on the evaluation of information gained through vendor interviews, ongoing client inquiries, reference checks and Gartner's knowledge of requirements in the market. Although the Magic Quadrant provides a picture of a vendor's Ability to Execute, as well as its Completeness of Vision, these factors should not be the only criteria for making a selection. Enterprises often use Magic Quadrants to formulate their shortlists and look only at vendors in the Leaders quadrant. Few enterprises will be successful finding the best vendor with this method.

Enterprises should determine their functional and support requirements and prioritizations, and they should use these to drive their selections. These requirements will be specific to individual enterprises and will be key for vendor evaluation and eventual selection. For example, a vendor in the Niche Players quadrant could be ideally suited to an enterprise's needs, because it may cost less and provide support for a narrower set of needs. Similarly, the vendors in the Leaders quadrant may have executed well and outpaced the market in vision, but this does not necessarily mean that they have the functionality needed to meet an enterprise's specific requirements.

Enterprises should understand that some solutions are better-suited for large businesses (those with more upfront complexity and reliance on problem management process maturity), and others are better-suited for small or midsize businesses (SMBs), because of their easier installation and lower cost, but, typically, fewer capabilities for complex event correlation. The Magic Quadrant is not designed as a substitute for client inquiry — Gartner inquiry is the best way for enterprises to resolve specific questions about event management vendors.

Figure 1. Magic Quadrant for IT Event Correlation and Analysis



Source: Gartner (December 2010)

As of December 2010

Market Definition/Description

ECA Products:

- Support the collection of events from elements in the IT infrastructure, including hardware, software, server, virtual machine (VM), operating system, network, storage, security, database, application and mainframe elements
- Process events using consolidation, filtering, normalization, enrichment, correlation, and statistical or model-based analysis techniques
- Notify the appropriate IT operations personnel of critical events

- Suggest remedial steps and, where possible, initiate corrective actions

Definition of Events

Two types of event categories need to be accepted and supported by ECA products:

- Discrete state changes in a managed element, sent asynchronously from the managed element, agents installed on the managed element, or another IT event-monitoring or ECA product.

- Threshold breaches indicating that a managed element is no longer operating within "normal" parameters, sent asynchronously from the managed element, an agent installed on the managed element or a separate performance-monitoring product. "Normal" can be based on a predefined, default and out-of-the-box threshold; a customer-defined, customized setting; or a dynamic, measured baseline.

(For a detailed description of the varying roles an ECA product can play in a potentially multitier event management architecture, see "Event Correlation and Analysis Market Definition and Architecture Description, 2010.")

Inclusion and Exclusion Criteria

To be included in this Magic Quadrant evaluation, a vendor must meet the following criteria for a single ECA product:

- At least 250 nonservice provider clients in production

- At least five reference accounts in the client base

- At least five clients actively monitoring more than 5,000 elements

- A product that was shipping as of December 2009

- Global sales and support on at least three continents

- The product must support the following functionalities:

  - Process both fault and performance events

  - Process events from two or more IT element types (e.g., server, network, storage, security, database or application)

  - Scale to more than 10,000 monitored elements

  - Have its own event collection mechanisms (e.g., agentry) and the proven ability (out-of-the-box) to integrate (bidirectionally) and consolidate events from third-party sources — e.g., fault-monitoring, performance-monitoring, application-performance-monitoring (APM) or behavior-learning tools — to fulfill an MoM role

  - Possess an automated, out-of-the-box ability to process/correlate events through two or more filtering/correlation techniques:

    - Deduplication/filtering

    - State-based correlation at the element level

      - Topology-based correlation

    - Correlation based on causal rules

  - Have the ability to present element and application event data to the IT operations staff

  - Be localized for the countries in which it is sold

Added

Zenoss has been added to the 2010 Magic Quadrant, based on client inquiries regarding this vendor. This is an indication that buyers see Zenoss as a player in the ECA market.

Dropped

Seven vendors have been dropped from this year's Magic Quadrant. Nimsoft was acquired by CA Technologies. Augur Systems, Interlink, OpenService (now LogMatrix), PerformanceIT, Sciencelogic and TNT Software did not meet the revised 2010 inclusion criteria.

Evaluation Criteria

Ability to Execute

The Ability to Execute (vertical) focuses on current product and market capabilities, representing Gartner's view of the strength of a vendor's corporate management, products, services and support, including its overall stability and viability. The ECA market includes several mature products from market-share-leading enterprise management vendors with large installed bases and robust cash flows. This sets the bar high for being placed in the Leaders and Challengers quadrants. However, revenue and customer count are not the only criteria for achieving a high Ability to Execute score.

Vendors with a strong Ability to Execute must have scalability and breadth of coverage to enable the collection of events across the entire IT infrastructure, including virtual servers and VMs. Vendors also must provide correlation functionality to reduce the event stream presented to the IT operations staff, including correlating events in light of the transitory nature of virtual versus physical relationships. However, customer experience shows that the more powerful the correlation tool and the more customization required to adapt the tool to a specific enterprise environment, the less likely an IT organization will be to successfully deploy it. Thus, ease-of-use and automation are key evaluation areas.

Gartner clients increasingly expect BSM capabilities (the ability to understand an event's impact on an IT service) to be an integral part of their ECA products. BSM links the availability and performance status of underlying IT infrastructure and application

components to business-oriented IT services that enable business processes. BSM has been a natural evolution from previous market requirements for event management and IT component monitoring, as IT organizations attempt to become more business-aligned in their service quality monitoring and reporting. However, progress toward this goal is impeded, because many event management customers are still struggling with the basics of providing instrumentation for the distributed infrastructure and enabling proactive monitoring. In addition, many do not have any end-to-end IT service definitions or documentation on how these relate to business processes.

Traditional general-purpose, rule-based event correlation engines are being challenged by new, focused vendors whose products are easier to deploy, because they have strong out-of-the-box functionality, although they typically have a limited ability to support customized event correlations. Customers are accepting the fact that the easy-to-deploy, cheaper, solution is "good enough," or they are using two tools: one for broad, but shallow, coverage of most of the IT infrastructure and one for deep, sophisticated correlation for a few critical components.

A product execution evaluation criterion on alarm thresholds explores vendor progress in simplifying deployment by automatically setting a baseline for the IT environment, dynamically setting variable thresholds and setting off an alarm only when current results deviate from normal baseline values. Reporting is another product execution criterion that is evaluated because this function can aid clients in monitoring and improving the event management process.

The size of the installed base, the number of new customers gained in 2010, and the strength of sales and marketing capabilities, along with the number of sales and support "feet on the street," contribute to a vendor's ability-to-execute ranking. We ranked the total installed base and growth in new customers separately, giving a heavier weighting to the number of new customers to distinguish a large, but possibly stagnant, customer base from a growing customer base. Industry partnerships through OEM relationships, value-added resellers and system integrators increase a vendor's ability to touch the market without increasing its internal investment in a direct sales force. Visibility in competitive situations and consistently making enterprises' shortlists demonstrate marketing credibility and brand awareness. Successful vendors match their marketing messages to the market's requirements and ensure that their direct and indirect sales channels, partnerships and alliances are effective.

During these challenging economic times, we have heavily weighted vendor viability, product execution and marketing execution in this ranking. Past consolidation and acquisition activity continue to wreak havoc with ECA vendors' portfolios; therefore, when determining a vendor's Ability to Execute, we evaluated customer experience, especially in terms of migration and graceful architectural change (see Table 1).

Completeness of Vision

On the Completeness of Vision (horizontal) axis, we evaluate how well a vendor or product will do in the future based on Gartner's scenario for where a market is headed, which we derive from our understanding of emerging technologies and the requirements of leading-edge clients.

Gartner evaluates how vendors' visions align with industry trends and evolving market requirements, their understanding of technical and market issues, their ability to differentiate products and grow their businesses, and their emphasis on best practices and the ease of deploying the event management solution, not just on product features. We examined build-versus-buy strategies for augmenting functionality, knowledge of core competencies and the ability to partner to fill gaps in the product portfolio. Industry perception and market recognition by prospects, partners and competitors based on a compelling and consistent marketing message is included. A vendor can succeed financially without a vision, but it will not become a leader without a clearly defined vision or strategic plan. This should include plans for articulating the vision and plans to differentiate the vendor's offering from competitors' offerings.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	standard
Overall Viability (Business Unit, Financial, Strategy, Organization)	high
Sales Execution/Pricing	high
Market Responsiveness and Track Record	standard
Marketing Execution	high
Customer Experience	standard
Operations	no rating
Source: Gartner (December 2010)	

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	standard
Marketing Strategy	high
Sales Strategy	low
Offering (Product) Strategy	high
Business Model	no rating
Vertical/Industry Strategy	no rating
Innovation	high
Geographic Strategy	low
Source: Gartner (December 2010)	

Under product strategy, we evaluate a vendor's potential for delivering continuous product innovation, advancing the state of the art in event correlation and automated root cause analysis, as well as its flexibility to adapt to changing requirements. ECA products do not stand alone in an enterprise management deployment. Vendors with strong product strategy visions demonstrate an understanding of and road maps for integration with other management applications and associated areas. These areas include the problem management process, e.g., the IT Infrastructure Library (ITIL) methodology and integration with the IT service desk tool; security information and event management (SIEM); configuration management databases (CMDBs; defined in this context as containing IT service relationship and dependency mapping information); APM tools; and the emerging real-time service models.

Higher vision rankings are accorded to vendors that have a credible strategy to achieve alignment between IT component events and business-oriented, end-to-end IT services. In the future, the ability to discover and document relationships between IT components and business services, as well as to keep the service dependency mapping updated in real time, will be necessary to automate the business impact analysis of events. Whether the service dependency mapping is documented in a BSM tool, a CMDB, a real-time service model or some other implementation entirely, it will not be possible to have an effective ECA without processing events against an up-to-date IT service dependency model to determine business impact and assign support priority.

The Completeness of Vision category also assesses vendors' product strategies for virtualization and cloud computing. These are key initiatives that demand that IT management tools be developed to address current needs and help IT organizations manage them successfully in the future. As part of the Magic Quadrant, we asked the vendors to clearly articulate their vision and strategy for managing these initiatives, then we evaluated them accordingly.

Leaders

Vendors in the Leaders quadrant possess a large and satisfied installed base and have a high degree of visibility in the market (for example, frequent consideration and success in competitive situations). They offer highly scalable, robust applications that can prioritize events to business impact, in both physical and virtual IT infrastructures. They must also have a strategic vision to address evolving enterprise requirements in the areas of IT service dependency mapping and optimizing the event-to-incident/problem resolution processes, including integration with service desk tools, APM tools and real-time service models.

Challengers

Vendors in the Challengers quadrant are solid and can perform well for many enterprises. Some are significant vendors in terms of size and financial resources, but may lack vision, deployability, ongoing innovation or an overall understanding of market trends.

Visionaries

Vendors in the Visionaries quadrant are forward-thinking and often technically focused. They have recognized and responded to longer-term event management market trends, such as root cause analysis and management of the virtualized environment. However, they may lack the recognition, sales and marketing strength, or the overall size to compete and execute with consistency.

Niche Players

Niche Players are a combination of new entrants to the event management market, vendors with limited vision or execution, and vendors that focus on a small segment of the market and do it well. The narrow focus reduces their vision ranking and limits their addressable market, making them unable to achieve a high Ability to Execute ranking. However, the narrow focus enables them to achieve great depth of functionality in their chosen areas.

Vendor Strengths and Cautions

Argent Software

Argent Software provides capabilities to midsize (or smaller) enterprise organizations and reports company growth and healthy increases in its installed base. According to customer references, Argent is one of a number of vendors providing a tool that is easier to implement and use without the complexity and cost of the larger software portfolio vendors. However, Argent is not a single product vendor — its Argent Advanced Technology product is supported by tools that monitor, collect and consolidate event data; discover network element information; and store the data in Argent's configuration database product, Atlas. In addition, the Argent Commander is a Web 2.0 interface to the Argent Advanced Technology suite that provides predefined "Command Modules," which enable IT organizations to go from a high level to server drilldown and visualize key performance indicators and event summaries of their IT infrastructure elements.

Strengths

- Argent provides a straightforward product addressing the needs of IT operations groups that lack the time, budget or need for larger, more-complex ECA products, while providing out-of-the-box value, including "Instant Best Practices." This provides Argent clients with immediate knowledge on how to set monitoring policy in line with best practices gleaned from Argent's global installed base.

- The Argent Advanced Technology product can monitor a broad range of IT elements, including virtual servers via a number of different architectures: agentless, agents or a hybrid combination.

- Although it is one of the smaller vendors in this Magic Quadrant, Argent has global coverage and support.

Cautions

- Argent focuses on providing an easier-to-use alternative to the larger software portfolio vendors, such as BMC Software, CA Technologies, HP and Microsoft; however, it will continue to find it increasingly difficult to differentiate itself, especially in the enterprise, as other vendors aggressively expand, integrate and consolidate their capabilities with adjacent tools areas, such as APM.

- Limited product depth means that Argent is used for its broad coverage across the wide variety of infrastructure elements with other tools (including other ECA tools included in the Magic Quadrant) used for deep analysis of critical devices.

- Argent is facing new competition from well-funded vendors entering the market with similar ease-of-use attributes, but more flexible go-to-market and business models, such as software-as-a-service, open-source and appliance-based offerings.

BMC Software

Due to the number of product changes and enhancements that BMC Software's ECA product has gone through, it's not surprising some clients can't name BMC's current ECA product, but are able to articulate the strategic direction the company is taking. Whether you're an BMC customer or are contemplating becoming one, it is useful to understand how BMC arrived at its current ECA offering, BMC ProactiveNet Performance Management (BPPM).

BMC's Patrol Enterprise Manager (based on the Boole & Babbage CommandPost technology acquired in 1999) was replaced by BMC Event Manager (based on a product called MasterCell, which was acquired with IT Masters acquisition in 2003 and split into two separate products — BMC Event Manager and Service Impact Manager). In May 2007, BMC announced its acquisition of ProactiveNet, a behavior learning technology tool vendor.

This year's Magic Quadrant product from BMC is BPPM, which combines the features from BMC ProactiveNet Analytics, BMC Performance Management (BPM, including BPM PATROL and BPM Portal), BMC Transaction Management Application Response Time (TM ART), BMC Event Manager (BEM) and BMC Service Impact Manager (SIM). BPPM is a convergence of all these products into a single, common platform and console for performance, availability, event and impact management.

BMC's customer experience execution and vision ratings continue to improve. This is the result of BMC's continual solidification of its availability and performance management tools functionality, its ability to deliver a solution that meets the needs of mainframe and distributed infrastructures, and its emerging capabilities for managing virtual IT environments.

Strengths

- Good breadth of coverage, including mainframe support, and the flexibility to use BMC's agent-based and agentless approaches, as well as other major vendors' agents.

- BMC achieved high marks for Completeness of Vision due, in part, to its innovative approach to monitoring, predictive root cause analysis and predictive service impact, supported by its end-to-end IT service management vision and its credibility to integrate its ECA product with other key IT operations management (ITOM) tools (e.g., service desks and CMDBs).

- BMC has differentiated itself and established thought leadership for ECA autobaselining, threshold analysis and anomaly detection, with the inclusion and integration of ProactiveNet.

Cautions

- Execution continues to lag marketing. In some cases, this results in products that aren't ready to meet their claimed values, or claims of results without setting the appropriate expectations around the required effort or required IT organizational maturity.

- Network management is only offered through a reseller agreement with Entuity or through integrations with other vendors products, such as Solarwinds' Orion or HP's Network Node Manager, resulting in the inability to draw profound information from the network infrastructure.

- Compared with HP and IBM Tivoli, BMC has a lower number of consulting and professional services resources. However, BMC's BPPM consultancy continues to grow globally.

CA Technologies

Since 2009, CA Technologies' Spectrum Infrastructure Manager (subsequently referred to as Spectrum) has been CA Technologies' Magic Quadrant ECA submission and strategic ECA product for the enterprise, replacing its longstanding CA NSM product. Spectrum also serves as CA Technologies' network device domain manager, which was its primary focus until Spectrum's role was extended to encompass servers and server software. Spectrum's enhanced role was accomplished by adding server-focused features and functions of CA NSM. In addition, Spectrum is enhanced by CA Spectrum Service Assurance (CA Technologies' BSM tool), which provides the ability to associate the IT infrastructure elements (using a service model) with IT services provided to the business.

As with all the ECA vendors with large tools portfolios, the value of CA Technologies' ECA tool is augmented when used in combination with other CA Technologies products, including CA eHealth Performance Manager (providing performance-monitoring data), CA Systems Performance for Infrastructure Managers (formerly CA SystemEdge) and CA Virtual Assurance for Infrastructure Managers (formerly CA Virtual Performance Management), providing instrumentation for physical and virtual servers.

CA's focus, investment and growth in ECA are strong, proven by its ongoing development of Spectrum, as well as the acquisition of Nimsoft in March 2010. Until the acquisition, Nimsoft NMS competed with Spectrum; however, CA Technologies has focused Spectrum as the enterprise ECA product with Nimsoft NMS focused on midsize enterprises. For the CA NSM enterprise

installed base, the road ahead remains one with options determined by the size and complexity of their IT infrastructure. Large enterprises will be led to migrate to Spectrum, with SMBs being directed toward Nimsoft.

Strengths

- Strong, out-of-the-box, model-based event correlation and root cause analysis capabilities.
- CA Technologies' improved execution rating is a result of its ongoing focus and investment in its ECA tool, release of BSM functionality, customer wins and the integration with synergistic CA Technologies tools that augment and enhance ECA in support of CA Technologies overall availability and performance management capabilities.
- The Spectrum companion CA eHealth Performance Manager product can provide a "deviation from normal" function, where thresholds are dynamically adjusted, using historical data to reduce alarm noise.

Cautions

- CA Technologies has experienced changes in its ECA portfolio. Therefore, as it continues to develop, enhance and integrate its ECA product lines, CA Technologies' prospects and clients should ensure their expectations and needs for ECA are met and are in line with CA Technologies' ECA product road map.
- It will remain a challenge for CA Technologies to keep its ECA tools (Spectrum and Nimsoft) focused on providing capabilities for two separate markets with overlapping needs. Failure to keep the tools differentiated will result in competing CA Technologies sales channels selling two products with significant overlapping functionality to the same clients, which may lead to confusion for CA Technologies' prospects and clients on what tools to choose.
- CA Technologies has a migration program in place, but it has not set a date for CA NSM customers to move to alternative tools; however, this type of activity is never painless.

eG Innovations

eG Innovations has been in the market since 2003, but has not gained significant market awareness and has a small, but global, customer base. Providing a mix of agentless and agent-based collection mechanisms, eG Innovations has broad element coverage, including support for virtual servers and desktops. eG Innovations reports its differentiations are its out-of-the-box root cause diagnosis (based on physical and virtual infrastructure dependencies without the need to build manually defined correlation rules), its ability to correlate how virtual servers support business services, and the capability to monitor virtual servers and desktops without agentry.

eG Innovations' references chose eG Enterprise Suite for its Citrix Systems support, ease of use, out-of-the-box correlation and thresholding. It also provided an alternative option to IT organizations considering Microsoft's Systems Center Operations Manager 2007. eG Innovations receives high marks for its vision, understanding, focus and capability to manage virtual server and desktop environments.

Strengths

- eG Innovations provides management of virtual IT infrastructures, including the ability to automatically detect and update application-to-VM mappings and VM-to-physical-machine relationships in real time.
- Its products supply the ability to observe a baseline of "normal" behavior and automatically set thresholds for each of the collected performance metrics, minimizing the incidence of false alerts.
- Flexible agent-licensing policy enable a single agent to monitor all the applications executing on a server. Agent licenses are not tied to operating systems or node-locked, enabling operators to pick and choose where they want to deploy the agents.

Cautions

- As with many of the smaller, emerging ECA vendors, eG Innovations' entry into large-enterprise accounts has been accomplished at the departmental level. This requires that large enterprises test to ensure eG Innovations can meet scalability and performance requirements.
- The service topology of interdependencies among applications, servers and devices that support a logical business service is not autodiscovered and must be created manually through a drag-and-drop interface. eG Enterprise can integrate with various CMDBs and IT service dependency mapping tools via internal application programming interfaces (APIs), but professional service efforts are required for this.
- Even though eG Innovations provides a tool with some integration with other tools (e.g., service desks), we do not see it used as the consolidation (MoM) event management tool to replace other complementary monitoring tools.

EMC Ionix

Although EMC sold many of its IT operations tools to VMware, the ECA products remain with EMC. EMC's Ionix Service Assurance Manager (SAM) is supported and augmented by add-on tools that provide dashboards, consoles, reports, event notification and support for specific IT infrastructure elements, protocols and software. EMC has successfully leveraged and extended the SAM "codebook correlation" model to EMC's storage domain. Other vendors have recognized EMC Smarts' excellence in this area, with Microsoft licensing a portion of the EMC Smarts technology to discover network topology and monitor network devices.

EMC's SAM can monitor a wide range of IT infrastructure components (server, storage and applications); however, its strongest play remains its ability to monitor the network (reflected in client inquiry and references provided by EMC). EMC's references indicated that SAM was effective at managing event data, especially processing large amounts of alarms and the ability to rapidly remove false alarms and identify the root cause. However, SAM is not a simple product, and attaining the product's value requires a high degree of skills to set up and use it effectively.

One concern is EMC's reliance on VMware's Integrien product as the only means of providing predictive analytics value to enhance and augment its ECA strategy. This dictates that any decision for the adoption of EMC's ECA strategy using VMware's products requires an understanding of VMware's product road maps to ensure the visions are aligned.

Strengths

- The EMC SAM's codebook correlation approach enables IT operations to discover topology relationships and to automate event correlation and root cause analysis without a significant amount of customization effort.
- EMC's deep network domain knowledge includes continuing development in new network technologies, such as voice over IP (VoIP), Multiprotocol Label Switching and native IPv6 environments.
- EMC's Ionix Server Manager, one of EMC SAM's domain manager products enhances SAM to provide the server and virtualization availability and performance management, enabling cross-domain correlation and impact analysis.

Cautions

- Although strong in network and storage, EMC Smarts shows no particular depth of domain knowledge in event management of databases and business applications.
- EMC depends on tools outside EMC's control to supplement, enhance and augment SAM's ECA capabilities.
- EMC continues to put marketing emphasis on extending the value of its ECA products to provide more business-oriented results — for example, EMC Ionix Business Dashboard; however, with a few exceptions, it remains predominantly a network management product (and network event consolidation point) in most production deployments, rather than being the overall MoM.

GroundWork Open Source

GroundWork Open Source's ECA product (GroundWork Monitor) was first released in September 2005. It is built on the Nagios open-source product, which brings in an open-source community that enables GroundWork users to benefit from enhancements that its community creates. GroundWork provides an alternative for IT organizations that would like the benefits of open source, but prefer to purchase a product with a support and maintenance contract. GroundWork provides support for a wide range of IT elements, and customers can also use adaptors developed through the Nagios exchange.

GroundWork is aimed at providing an alternative to larger and more established ITOM vendors; however, it's primarily being adopted by companies with small-to-midsize IT infrastructures. Gartner clients and vendor references indicate that, even though the benefits of open source include a low-cost tool with constant development and enhancements from the open-source community, it remains complex to use, product usability (interfaces) need to be improved and plug-ins (integrations with components) need frequent updating.

Strengths

- GroundWork provides open-source products integrated and supported by a commercial ITOM vendor.
- Enhancements are created 24/7 by the open-source development community.
- GroundWork's ECA capabilities are offered at low prices.

Cautions

- Taking full advantage of GroundWork requires that a technically savvy user and an IT operations organizations be familiar with open-source communities.
- Groundwork depends on the open-source community for adapters and product enhancements.
- Upgrades can be tricky, because homegrown product enhancements and community developments need to be documented and supported by users.

HP

HP continues to invest in its Operations Center suite of products, especially ECA. HP's aim has been to simplify its tools' positioning, usage (implementation, setup, administration and integration with complementary ITOM tools) and pricing. Operations Manager i (OMi) sits on top of HP Operations Manager (OM), fulfilling an MoM function, taking the events data from OM (or other domain managers) and providing topology-based event correlation. HP's Operational Data Model, released in 2008, has had a name change and is now called the Run-Time Service Model (RTSM). It is delivered via OMi and is now available to all Operations Center clients. HP's RTSM is designed to provide a single mechanism for the element discovery and data collection used by OM, Business Availability Center, and Network Node Manager i. OMi uses inputs from the event streams and RTSM to identify the cause of incidents.

For those who do not keep up-to-date with HP's software strategy and road map, product changes and additions continue to result in end-user confusion — requiring a "you are here" map for portfolio navigation. Nonetheless, HP continues to demonstrate how ECA functionality augments, enhances and leverages other IT management areas, including APM, BSM, problem management, CMDB and storage management.

The results of HP's ECA simplification efforts have not yet been mentioned by Gartner clients or HP references — many IT organizations still require dedicated expertise and services to plan, implement and set up the tools. HP has changed the way it licenses its agents, moving from a tier-based pricing model (price based on server hardware capacity) to a license based on a single operating system (physical or virtual). This is a positive move by HP, because it simplifies purchasing. However, depending on the IT infrastructure, there's no guarantee this will translate to a lower cost. The single price agent spans operations and performance, and includes Sitescope agentless monitoring.

Strengths

- HP's ability to apply OM to meet the latest virtualization challenges is strong (e.g., as demonstrated with HP's new virtualization SPI), delivering customer satisfaction and showing that HP has the ability to keep up with today's challenges.
- HP's OM continues to have the second-largest installed base (behind only Microsoft) and consistently appears on enterprises' shortlists, demonstrating credibility and market awareness.
- HP has built out-of-the-box domain knowledge into its agents to filter and correlate local events, based on predefined policies and default thresholds, along with the templates for automated corrective actions aimed at reducing human effort and implementation time.

Cautions

- Even though HP has introduced "starter bundles," which are aimed at midsize IT organizations, HP's enterprise ECA products require a monetary and labor investment that is generally too large for midsize IT organizations looking for basic ECA capabilities.
- HP continues to change and update its portfolio, making it challenging to understand its road map and plans. This makes tool comparisons and strategic investment decisions difficult.
- As with previous years, HP's list pricing for a Gartner-provided sample configuration was the most expensive of all the ECA quotes, although HP states that customers would receive significant volume discounts off list price.

IBM Tivoli

IBM Tivoli's ECA product, OMNIbus v.8.2 (originally released by Micromuse in 1995), has not had any major enhancements or changes for years. IBM's strategy for ECA focuses on providing tools that augment and enhance the core OMNIbus product. This includes the addition of the IBM Tivoli Data Warehouse (TDW) to create reports showing how faults or change events affect performance, a limited-use license of IBM Tivoli Netcool/Impact to enrich events, manage maintenance windows, integrate multiple data sources and build a foundation for IT operations process automation, i.e., run book automation (RBA); IBM Tivoli Monitoring (ITM) for monitoring and analysis of the OMNIbus object server and the operating system where it runs; and the IBM Tivoli Common Reporting (TCR) to provide reporting across multiple products and domains.

Although the core OMNIbus features and functions remain relatively unchanged, IBM Tivoli has included out-of-the-box monitoring templates and out-of-the-box integration with other products in its suite of monitoring tools. These include IBM Tivoli's BSM product, which provides event processing against a service model to determine the service impact. IBM Tivoli's OMNIbus offers one of the broadest IT infrastructure element (hardware and software) coverage capabilities in the industry and we continue to see IBM Tivoli OMNIbus used as an MoM, because of its strong scalability and its broad and deep capabilities to integrate and consolidate data from a wide range of IT components and third-party management products.

IBM's references for this Magic Quadrant were large enterprises with large and complex IT infrastructure using OMNIbus to monitor their servers, networks, middleware, databases and applications, either directly or through integration with a lower-level, domain-focused event monitor.

Strengths

- IBM has the broadest coverage in the Magic Quadrant, as regards depth of ECA capabilities across server, network, application, database, storage and mainframe and agentless monitoring alternatives for some operating systems, leveraging Simple Network Management Protocol, Common Information Model and Windows Management Information technology.
- IBM continues to extend its ECA capabilities by providing IBM TDW and IBM TCR at no additional cost to provide analysis and reporting for event trending and performance monitoring.
- IBM Tivoli provides automated baselining to create bands of normalcy around various periods of time (time of day, on-shift, after hours, etc.) and compute dynamic thresholds as a standard deviation or percentage variance from normal to reduce the number of non-action-oriented alerts.

Cautions

- Although IBM Tivoli has introduced a low-end Event and Network Management product, solving difficult ECA problems for large customers requires complexity and cost in the solution — not just the software license cost, but also the cost of deployment and ongoing cost of administration.
- IBM Tivoli's plans for OMNIbus, (e.g., ongoing support for managing the increasingly complex virtual infrastructure) contributes to its vision position in the Magic Quadrant, which must be monitored carefully (e.g., by tracking ongoing enhancements against a published product road map). Beyond improvements in scalability and interoperability with IBM and non-IBM products, the core OMNIbus product has not been enhanced greatly since it was acquired in February 2006 as part of the Micromuse acquisition.
- IBM Tivoli's multiple acquisitions have brought IBM a large product portfolio, but has left it with a complex portfolio and multiple architectures that IBM Tivoli continues to rationalize and integrate as a high priority. However, this can make it challenging for their sales organization to articulate IBM Tivoli's value proposition and has left some buyers unclear about the company's long-term strategy and vision.

Microsoft

System Center Operations Manager 2007 R2 (OpsMgr R2) is Microsoft's latest ECA product release. OpsMgr 2007 R2 has increased its features and functions, providing a range of capabilities in a single product, including fault and performance monitoring and synthetic transaction monitoring, a single view for physical and virtual servers, and Windows and Linux operating systems (Linux requires a third-party OpsMgr 2007 management pack), as well as integrated service-level monitoring. OpsMgr's features and functions are not unique, compared with other ECA products; however, its solid capabilities for managing Windows Servers in conjunction with its low price will continue to apply competitive pressure, especially in companies with large Microsoft Windows infrastructures. Microsoft's investment in management software is driven by its desire to reduce the total cost of ownership of the Windows operating system and Microsoft applications.

Microsoft's OpsMgr predecessor, Microsoft Operations Manager (MOM), was primarily aimed at the systems administrator managing small numbers of Windows servers. However, OpsMgr has succeeded in providing an ECA product for the enterprise that supplies capabilities (including scalability and performance) provided by more-established and expensive ECA tools. Enterprises of all sizes may find the move to OpsMgr of value; however, it may be too complex for IT organizations in the midmarket, and SMBs may seek simpler alternatives. Expect Microsoft to continue to enhance and augment OpsMgr with other tools in the System Center suite, which will include integration, with Opalis providing automation for root cause and remediation and integration with the Avicode acquisition, enabling Microsoft to provide an element to the .NET transaction view.

Strengths

- Microsoft OpsMgr has the largest ECA installed base (although not the largest revenue), and this has contributed to Microsoft's Ability to Execute ranking.
- Companies with a large and growing investment in Microsoft Windows servers are actively investigating OpsMgr as an MoM. Conversely, in companies with a heterogeneous IT environment, OpsMgr is used by Windows systems administrators and is typically deployed as a subordinate in a hierarchical event management architecture, passing Windows events up to a broader, general-purpose, multivendor event console.
- Gartner clients and references have described OpsMgr as a reliable, cost-effective product that provides good physical and virtual server management capabilities. Microsoft also provides support for non-Microsoft platforms, such as Linux, Unix and VMware.

Cautions

- Microsoft continues to lean heavily on its partners to fill some major holes in its product coverage (e.g., monitoring of hardware, storage and non-Microsoft software, including applications, middleware and databases). This introduces complexity (administration, etc); costs (software, maintenance and potentially another product requiring additional skills); and risk (another vendor with its own support, road maps and priorities) into the equation.
- Gartner clients have informed us that the move from MOM to OpsMgr 2007 can require more effort (e.g., to define and implement the more-sophisticated tool architectures). It may also introduce scalability challenges and require a higher level of skills and expertise.

- Microsoft licenses OpsMgr as part of the System Center suites (data center or enterprise), meaning IT organizations seeking a stand-alone ECA purchase from Microsoft will need to invest in the entire Microsoft Systems Center suite.

NetIQ

NetIQ's AppManager first made an appearance in 1997. AppManager is part of the NetIQ AppManager Suite, which includes 65 modules for monitoring systems, network devices, applications and end-user experience monitoring. Hence, it is not specifically focused on ECA; it is treated more as a foundation function to support its core competencies of application and operating system management. Nonetheless, NetIQ continues to augment its NetIQ AppManager product, including expanding the NetIQ AppManager Performance Profiler (AMPP) template library of out-of-the-box correlation logic by adding new templates for VMware, Web response time and network devices, as well as fully integrating NetIQ's Aegis, its process automation product.

The AMPP templates automatically baseline the environment, measuring application performance metrics continuously to determine the normal range, and provide dynamic thresholding, comparing current performance against the normal workload range to determine anomalies. NetIQ has a large installed base, and, although the number of licensed modules continues to grow, overall license revenue has declined, partially due to price erosion from increased competitive pressures, especially from Microsoft. As a result, NetIQ has continued to enhance its product, providing support of VMware, VoIP and the emerging unified communications market. It has also integrated automation (via NetIQ Aegis) into the product for root cause analysis and to support integration with other tools — e.g., service desks to support the incident-to-resolution process.

Strengths

- Some innovative ECA functions are included in NetIQ AppManager, such as using conditional logic at the agent level to perform multiple checks, validate errors and reduce the number of events generated for a single problem.

- NetIQ AppManager for VMware provides a visually pleasing holistic view of the virtual infrastructure, highlighting when one virtual server may affect others, including instances of consuming resources beyond its allocation, and the impact that virtual servers have on the applications running on the VMs.

- NetIQ has successfully integrated its IT operations process automation (i.e., RBA) product, NetIQ Aegis, with NetIQ AppManager, enabling users to extend its value to automate fault management processes (such as root cause analysis and fault-to-remediation).

Cautions

- NetIQ is not specifically focused on ECA from an MoM perspective and is typically deployed as a domain specialist in the middle tier of a three-tier event management architecture. It then feeds results up to a broader, general-purpose, multivendor event console.

- NetIQ's innovation has been diverse, with a focus on areas such as IT operations process automation and the monitoring of virtual infrastructures receiving a great deal of attention. Integration with CMDBs and IT service dependency mapping tools has received less. This demands that clients and prospects understand NetIQ's strategic focus to ensure that its priorities and deliverables are aligned with theirs.

- Customer references report that the value NetIQ AppManager provides in terms of in-depth detail requires intimate product knowledge to deal with the complexity. However, some level of complexity is necessary to enable the positive attributes of flexibility and customizability of the product.

Quest Software

Quest Software does not specifically focus on ECA, but it invests in it as a foundation function to support Quest's performance and APM tools and to help IT operations teams bridge the gap between infrastructure and transactional monitoring. Quest's ECA product, Foglight, uses a combination of agent-based and passive network packet capture technology to gather data directly from the IT environment. It is designed to impose a minimal overhead on the monitored host. Foglight also comes with adapters that enable data to be imported from other management systems and environments.

Quest's ECA innovations are focused on making its foundation an open architecture, with an exposed service layer that customers, Quest professional services and Quest engineers can leverage to monitor data, build browser interfaces, and create rules logic using Groovy scripts — a scripting language for the Java platform chosen by Quest to avoid creating a proprietary scripting language.

Strengths

- Quest has invested in applying ECA to the virtualized environment, providing visibility into the combined health of the physical host and guests within a single view. If there's a problem with a physical host, Foglight can identify which guests are affected and vice versa.

- Quest demonstrates a good understanding of dynamic thresholding and pattern recognition, using moving averages and standard deviations off a baseline.

- Customer references indicate that the out-of-the-box reporting capabilities help fine-tune thresholds, improving the event management process. A graphical-user-interface-based report builder can be used to create customized reports.

Cautions

- Quest is not specifically focused on ECA from an MoM perspective, and Foglight is generally deployed as a domain specialist in the middle tier of a three-tier event management architecture. It feeds results up to a higher-level MoM, such as HP Operations Manager or IBM Tivoli Omnibus.
- Quest's list pricing for a Gartner-provided sample configuration was the second most expensive of all the ECA quotes; however, Quest plans to repackage Foglight to provide more-flexible pricing options.
- Although Quest gets credit for some well-stated strategies for CMDB — where IT service dependency models are leveraged to assess business impact from IT events — manual relationship mapping is required to document the service chain.

Tango/04

In addition to ECA, Tango/04 also provides BSM and SIEM. Managing IT in line with the business services is a key focus for Tango/04 and aligns with the ambitions of many enterprise clients needs; however, although Tango/04 is starting to be adopted by larger enterprises, Tango/04 is typically used by SMBs in Europe and Latin America (where the company is called Barcelona/04 due to trademark issues with the Tango name there). Its small customer base constrains its Ability to Execute ranking. Tango/04 provided a wealth of client references which mentioned that the reasons for purchasing Tango/04 were rapid deployment, ease of use, cost, and BSM and SIEM integration.

Strengths

- Tango/04's Visual Message Center product is used more often for BSM than for infrastructure or component-focused ECA. Some customer references have extended beyond BSM to business process alerting and service-level management.
- Tango/04 presents real-time, dynamic calculation of the business impact cost of a component incident to the operator to better prioritize support resources, without the need to define weights or costs for each component.
- Tango/04 has a strong strategy and vision relative to security event integration, with many production deployments already incorporating SIEM.

Cautions

- Tango/04 has limited global sales and support. It is focused on Europe and Latin America (predominantly, Brazil and Argentina), and I just beginning to invest in North America.
- The IT service model required for BSM and event impact analysis is constructed manually through drag-and-drop editing. Tango/04 believes that CMDB tools will never be mature enough to be a basis for BSM projects; thus, Tango/04 does not plan to import IT service relationship and dependency mapping information from CMDBs, considering them inhibitors to agility and rapid ROI.
- Although Tango/04 supports virtual servers, it lacks the dynamic sophistication found in other ECA tools. Providing new differentiating virtualization capabilities will remain a challenge.

uptime software

Uptime software first appeared in "Magic Quadrant for IT Event Correlation and Analysis" in 2009. The company's up.time product was first released in 2001. Uptime has a healthy, growing customer base selling mainly to the SMBs, and the up.time product is not used as an MoM. Instead, it can provide division-level management capability, reporting to an MoM in a large or distributed IT infrastructure. Up.time is one of a growing number of ECA products that combine fault and performance monitoring, enabling it to provide availability data to address immediate issues and issues of service degradation. It also has good capabilities for managing virtual server environments, including the ability to show, in one holistic view, how each virtual server is affected by the physical server (e.g., percentage use over a period of time). It also provides bidirectional integration with VMware's vOrchestrator to automatically trigger actions.

Uptime's ability to differentiate, attract channel partners and meet rapidly evolving market requirements (e.g., business service aligned availability management) will remain a hurdle for this still-emerging vendor. This factor will determine how successful up.time will become in a highly competitive market.

Strengths

- Up.time provides a combination of fault and performance management.
- Uptime's pricing is attractive.
- It has a distributed architecture.

Cautions

- Although uptime continues to innovate and differentiate itself, it is operating in a highly competitive market.
- With a small number of exceptions, up.time's adoption by enterprises has been accomplished through departments that require the largest IT infrastructures to test and ensure that up.time can meet their corporate data center scalability and performance requirements.
- Integrating with other ITOM tools in support of key IT operations initiatives (e.g., IT service desk, CMDB and APM tools) could be an issue.

Zenoss

Zenoss is the new entrant to the 2010 Magic Quadrant. Founded in 2005, the Zenoss ECA product, Zenoss Enterprise, is one of a new-breed of IT operations tools vendor providing what has become known as a commercial, open-source product. Like GroundWorks, Zenoss provides an open-source tool with levels of maintenance and problem support. Unlike GroundWorks, which bases its tool on the Nagios open-source product, Zenoss developed its own platform. As with an increasing number of ECA tools, Zenoss Core (free) and Zenoss Enterprise (fee-based) monitor faults and performance for servers (physical and virtual), networks and applications.

Zenoss has what it calls a real-time service model, which provides logical and physical grouping, enabling devices to be manually mapped to business systems, locations and people. The model is populated and maintained by an autodiscovery process, supplemented by a Web services API, XML import/export or manual user input.

Device and software support and tools integration are accomplished with add-on Zenpacks (provided by Zenoss and developed by Zenoss and the open-source community). Unlike Zenoss Core, Zenoss Enterprise comes with increased functionality (e.g., greater monitoring capabilities for servers and applications) integration with other ITOM products, higher scalability, role-based security and product support. It is licensed with three pricing and service plans (Silver, Gold and Platinum).

Zenoss has been successful in attracting a growing installed base in a relatively short period of time Gartner clients and vendor references mention pricing, speed of deployment and functionality (especially for managing virtual environments) as the primary reasons for choosing Zenoss. However, reporting and information presentation were seen as areas in need for improvement.

Strengths

- Zenoss provides a product with good ECA features and functions, as well as a strong capability for monitoring virtual infrastructures at low prices.
- This is a single, multidiscipline product supported by a commercial ITOM vendor.
- Enhancements are created 24/7 by the open-source development community.

Cautions

- The value of commercial open source is not enough to differentiate and gain adoption, which requires Zenoss to continue innovating and developing its product to meet some of today's more-challenging IT infrastructure environments.
- Zenoss depends on the open-source community for adapters and product enhancements not provided by the vendor.
- Upgrades can be tricky. Homegrown product enhancements and community developments need to be documented and supported by the user.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all pre-sales activities and the structure that supports them. This includes deal management, pricing and negotiation, pre-sales support and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.