Magic Quadrant for Security Information and Event Management

Published 19 October 2021 - ID G00471487

By Pete Shoard, Andrew Davies, and 1 more

Security and risk management leaders continue to need a security system of record with comprehensive threat detection, investigation and response capabilities. SIEM is evolving into a security platform with multiple features and deployment models. This research will help you find the right solution.

Learn how Gartner can help you succeed
Become a Client

Market Definition/Description

SIEM aggregates data from log and event data for monitoring, assessment, detection and response enabling advanced across application, network, endpoint and cloud environments. Capabilities include collection, storage, normalization, correlation, analytics, visualization, and incident response to concerns/ managed through security orchestration, automation and response (SOAR). Security reporting and continuously updated threat content through threat intelligence platform (TIP) and threat hunting capabilities are also included. Deployment options include software, cloud service, or fully managed or managed services.

Magic Quadrant

Figure 1: Magic Quadrant for Security Information and Event Management

Leaders
Challengers
Visionaries
Niche Players
Vendor Strengths and Cautions
Devo
Devo is a Challenger in this Magic Quadrant. Its SIEM product, the Security Operations application, is delivered as a SaaS offering. Devo's SIEM customer base is primarily in North America, followed by Europe, the Middle East and Africa (EMEA) and Asia/Pacific (APAC) and Japan (APAJ). Its customer base is split almost evenly between large and midsize enterprises, and its product has a strong appeal to midsize enterprises and organizations with limited security staffing. Devo's SIEM offering is a cloud-native platform that ingests, normalizes, stores, analyzes, and visualizes security operations data. Its Security reporting and continuously updated threat content through threat intelligence platform (TIP) and threat hunting capabilities are also included. Its Security reporting and continuous service, it has support for automation.
Magic Quadrant
Figure 1: Magic Quadrant for Security Information and Event
Strengths
Devo's SIEM is a cloud-native platform that ingests, normalizes, stores, analyzes, and visualizes security operations data. Its Security reporting and continuous service, it has support for automation.
Cautions
Devo's SIEM is a cloud-native platform that ingests, normalizes, stores, analyzes, and visualizes security operations data. Its Security reporting and continuous service, it has support for automation.

Splunk

Splunk is a leader in the Magic Quadrant. Its Splunk Enterprise Security Suite (ESS) and its addition to the Splunk Enterprise solution. It is important to note that Gartner does not assess or rate the core Splunk Enterprise platform, only the ESS and Splunk Cloud Platform. Splunk's ESS and Splunk Cloud Platform offerings are based on Splunk's SIEM and large analytics capabilities. The direction of Splunk ESS to offer more assessment of assets and identities through its AI and promise more content delivery (containing a variable on-release day or cloud schedule) indicated by its "Splunk Enterprise Security".

Strengths

Security-focused roadmap. The SaaS model of Splunk ESS includes TAP and UEBA capabilities as no additional cost. Historically, Splunk has been a product-focused model and vendor. Splunk's new packaging critical components with Splunk's ESS to deliver a more comprehensive security solution.

IT observability coupled with security: A continuing advantage for Splunk is its ability to deliver IT observability and security capabilities in a single platform. Customers can leverage Splunk Enterprise Security ESS to security teams. Splunk is increasing the future of environments with Splunk Observability Cloud and Splunk Enterprise Security ESS.

Security operation user experience: Buyers of Splunk consistently report positive user experience with the product on proven query functionality, API capabilities, customized dashboards and alert science-based analytics provided out of the box.

Cautions

Pricing: Buyers are reporting angst with Splunk costs and their ability to forecast future costs. Customers are looking for more transparency in Splunk's pricing and are considering leaving existing Splunk clients and key buyers plans to look at cheaper alternatives in offset future licensing migration and storage costs.

Complexity and expertise: Buyers express trepidation about the complexity of Splunk ESS and existing users communicate problems with data management within the solution. There are also real concerns about the ability to find Splunk talent. Splunk's ESS is not the most "turnkey" or comprehensive between owners of Splunk ES in the Ferrie latest post.

Regional sales expertise: The majority of Splunk's salesforce is based in North America, with a smaller sales and marketing presence outside the region. Lack of regional sales and support experiments and customers can lead to poor experience from a sales and support perspective.

Sumo Logic

Sumo Logic is a Visionary in the Magic Quadrant. Its SIEM product, Cloud SIEM, is delivered as a SaaS offering and is based on its cloud-native platform. Sumo Logic's Cloud SIEM is a cloud-native solution with the ongoing launch in North America. The company has increased its presence in the Europe and Asia/Pacific regions over the past year. In 2021, Sumo Logic acquired DFLabs, which provides security automation capabilities. Sumo Logic's Cloud SIEM provides security analytics and information security with a similar efficacy to a stand-alone SIEM offering. Licensing is attractive based (with pricing based on data ingestion) or credit-based (with credits being used to enable specific capabilities, such as UEBA or vulnerability assessment or continuous validation). Sumo Logic's strengths are:

Strengths

Tactics and DevOps orientation: Sumo Logic's core-oriented beyond security operations use cases into development and operations, which is the company's heritage, and demonstrates the data analytics capabilities.

Free assessment of the stack: Sumo Logic provides threat intelligence on CloudSiteScan additional environment at no added charge.

Integrated SOAR functionality: DFLabs SOAR capabilities are now assimilated into the SIEM pure acquisition, which includes time-consuming DevOps tasks as well as the time needed to deploy on SOAR and has the integration needed to make it functional.

Cautions

Analytics maturity: Sumo Logic does not have the breadth of advanced analytics capabilities, such as UEBA, which compared to other SIEM offerings is a disadvantage.

Operating expenses: Revenues on Gartner's Peer Insights have expressed concerns around Sumo Logic's operating expenses, specifically impacting performance when searching for large data sets.

Limited visibility: Although Sumo Logic's Cloud SIEM provides access to MITRE ATT&CK protections in terms of identifying advanced SIEM support, its third attack for SIEM among and over Gartner criteria remains the.

Vendors Added and Dropped

We review and adjust our inclusions criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may indicate a change in our business practices, but it may also be the result of a change in focus by that vendor.

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may indicate a change in our business practices, but it may also be the result of a change in focus by that vendor.

Added

- Gartner Peer Insights customer and Functional requirements for inclusion in the 2022 Magic Quadrant for SIEM

Dropped

- Venus Tech did not meet functional and commercial requirements for inclusion in the 2022 Magic Quadrant for SIEM
- FireEye combined with Mandiant as acquisition to form FireEye and did not meet commercial requirements for inclusion in the 2022 Magic Quadrant for SIEM
- McAfee combined with FireEye as acquisition to form FireEye and did not meet commercial requirements for inclusion in the 2022 Magic Quadrant for SIEM
- Odyssey did not meet commercial requirements for inclusion in the 2022 Magic Quadrant for SIEM
- Micro Focus did not meet Gartner Peer Insights customer and functional requirements for inclusion in the 2022 Magic Quadrant for SIEM

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that Gartner analysts considered necessary for a vendor to be included in this Magic Quadrant.

To qualify for inclusion, a vendor needed to fulfill the following criteria:

- A product that provides SIM and SOAR capability in and-alert correlation into cloud-native software and/or SaaS.
- Features, functionality and add-on solutions including at least two of the below named additional capabilities that were generally available, vendor-owned (wholly acquired or organically built) and included in the SIEM product or sold as standard add-on as of 1 February 2022:
  - Security orchestration, automation and response (SOAR)
  - Threat intelligence platform (TIP)
  - User and entity behavior analytics (UEBA)
  - Long-term storage and reporting (greater than 365 days)
- A product that supports data capture and analysis from heterogeneous, third-party sources via API in addition to data streaming or log collection (that is, other than from the SIEM vendor's products/SaaS), including network-based technology, endpoint/servers, cloud (laaS or PaaS), identity and access management (IAM) and business-critical applications, delivered with at least 10 major security technology vendors.
- Cloud-native SaaS licence and maintenance (including managed services) revenue exceeding $50 million in 2021 (including Managed Security Services [MSS] and managed detection and response [MDR] services) and a minimum of 50 paid customers as of the end of that same year.
- In the 12 months prior to February 2022, it has received 15% of SIEM cloud-native/SaaS revenue from buyers with headquarters outside the geographical region of the vendor's headquarters location, or having at least 20 production customers, each with headquarters outside the geographical region of the vendor's headquarters location.
- Sales and marketing operations (no provisional campaigns), local language technical support, and sales/marketing investments (primarily in-person selling/marketing) at least two geographical regions as of 1 February 2022.

Excluded from consideration were:

- Capabilities available only through a managed services relationship — that is, SIEM functionality available to customers only when they sign up for a vendor's managed security, or managed detection and response, service. Gartner does not consider managed security services, or managed services, as more than a vehicle that organizations engage the vendor to establish, monitor, escalate and/or respond to alerts, incidents and cases.

Honorable Mentions

- **Zenoss** was not assessed in prior Magic Quadrants for SIEM Gartner analysts, however it is considered because of its ability to deliver customer clients due to its cloud native architecture, big processing capabilities and visualizations. Zenoss's strengths are its flexibility, ease of use, and its ability to deliver customer clients due to its cloud native architecture, big processing capabilities and visualizations. Zenoss's strengths are its flexibility, ease of use, and its ability to deliver customer clients due to its cloud native architecture, big processing capabilities and visualizations.
- **Gigaspaces** did not meet the functional requirements for inclusion in this Magic Quadrant. Gigaspaces's product, XDR, which had started with proprietary infrastructure and application monitoring, and then began offering support for security operations use cases. It now offers Gigaspaces Security, which provides security analytics and SIEM capabilities. Gigaspaces's strengths are:
- Gigaspaces's product, XDR, which had started with proprietary infrastructure and application monitoring, and then began offering support for security operations use cases. It now offers Gigaspaces Security, which provides security analytics and SIEM capabilities. Gigaspaces's strengths are:

Gigaspaces's product, XDR, which had started with proprietary infrastructure and application monitoring, and then began offering support for security operations use cases. It now offers Gigaspaces Security, which provides security analytics and SIEM capabilities. Gigaspaces's strengths are:

- **Google Chronicle** was not surveyed as part of this Magic Quadrant. Chronicle has an obvious native security information and event management (SIEM) offering, which is based on its cloud-native platform Cortexed Gartner. Chronicle is capable of large-scale log search and offer least-expensive pricing. As a result of the acquisition of Siemplify, Chronicle can now be coupled with SOAR functionality.
- **Fortinet** did not meet the commercial requirements for inclusion in this Magic Quadrant. Gartner's offers a cloud native detection as code platform as a SIEM alternative for cloud-focused linear security operations. Fortinet's SIEM offering is a combination of Fortinet's FortiSIEM and also offers a secondary architecture and is fully managed by its support team.

Evaluation Criteria

Ability to Execute

Product or Service: This criterion evaluates a vendor's ability to provide product functions in core SIEM areas such as the ability to create, modify and maintain threat detection use cases, provide case management, provide security automation activities and generate reports to support compliance and threat hunts.

Overall Viability: This criterion includes an assessment of a vendor's customer traction, the financial and practical success of the SaaS SIEM business, and indicators that it will continue to invest in SaaS technology.

Sales Execution/Pricing: This criterion evaluates a vendor's success in the SIEM market and its capabilities in presales activities. Considerations include the size of its SIEM revenue and installed customer base, the quality of its customer references, the ease of the RFP process, the quality of sales support, and the distribution and productivity of its sales channel. The level of interest and received responses from Gartner clients is also considered.

Market Responsiveness/Record: This criterion evaluates the ability to respond, change, or adapt to client demands in regard to product capabilities and business model in relation to what the market wants of SIEM. Considerations include support for multicloud monitoring, cloud-native or SaaS-delivered SIEM, and the ability to deliver on customer requirements.

Marketing Execution: This criterion evaluates a vendor's SIEM market messaging in light of Gartner's understanding of customer needs. It also identifies particular vendors identified variations by industry or geographic segment.

Customer Experience: This criterion evaluates product function and service experience in production environments. Included are, operations, administration, and vendor support capabilities. This criterion includes the ease of the RFP process, the quality of sales support, and the quality of the customer account relationship with Gartner clients that are using, or have completed competitive evaluations of, a vendor's SIEM offering.

Operations: This criterion evaluates a vendor's service, support and sales capabilities. It includes an assessment of these capabilities across multiple geographies.

Table 1: Ability to Execute Evaluation Criteria

Image Table ⊡

Evaluation Criteria ↓	Weighting ↓
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	Medium
Operations	Medium

Source: Gartner (October 2022)

Completeness of Vision

Market Understanding: This criterion evaluates a vendor's ability to understand buyers' emerging needs and how to communicate solutions effectively. SIEM vendors that show the highest degree of market understanding are those that are able to provide a roadmap for the future that addresses emerging security capabilities requirements, while also meeting the business risk and RFI reporting needs of organizations.

Marketing Strategy: This criterion evaluates a vendor's ability to communicate the value and competitive differentiation of its SIEM offering.

Sales Strategy: This criterion evaluates a vendor's use of direct and indirect sales, marketing, services, and communications affiliates to extend the scope and depth of its market reach.

Offering (Product) Strategy: This criterion evaluates a vendor's approach to product development and delivery with an emphasis on how well functionalities and features correspond to current requirements and future trends in the SIEM market. This includes the ability to meet the needs of SIEM buyers. There is little differentiation between most vendors in areas such as support for common network devices, security devices, OSs and conventional administration capabilities. We assign higher weightings to coverage of emergent/niche security capabilities, such as SaaS and cloud administration.

Business Model: Despite vendors' focus on expanding their capabilities, we continue to value sound business models. We value vendors that have demonstrated a commitment to the security market and security research and value the attributes over breadth of coverage/depth based upon cases. SIEM products are complex and tend to become more so as vendors extend their capabilities. Vendors data collection capabilities are a critical component of their business model. We value vendors that have leverage with hardware vendors — will be the root cause/RCA, the evaluate capacity to monitor and the fastest deployment of SIEM technology and supporting services, because growing numbers of Gartner clients are looking for managed security services (MSS) and managed detection and response provider partner capacity for monitoring or managing the SIEM technology deployments.

Vertical/Industry Strategy: This criterion evaluates a vendor's strategy to support SIEM requirements specific to industries, the operational technology (OT) environments.

Innovation: This criterion evaluates a vendor's development and delivery of SIEM technology that is differentiated from that of the competition in a way that uniquely meets customers' most important requirements. Innovation can be in areas such as support for cloud-native SIEM, support for identity-oriented monitoring and incident investigation and response. This is in addition to other capabilities such as UEBA, security orchestration, automation and response (SOAR), and threat intelligence purpose-built capabilities related to advanced threat detection and incident response, user, data and application monitoring, ad-hoc queries, visualization, orchestration and incorporation of content to investigate incidents, and workflow-based management.

Geographic Strategy: This criterion takes account of the fact that, although the North American and European markets are the most developed markets for SIEM, other regions, such as Asia/Pacific and Latin America, are growing their capacity to provide security services to their customers. This criterion also considers the Critical Capabilities for Security Information and Event Management, which may include off-cycle updates, to ensure that we vendors meet significant security requirements in Critical Capabilities for security operations.

Table 2: Completeness of Vision Evaluation Criteria

Image Table ⊡

Evaluation Criteria ↓	Weighting ↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (October 2022)

Quadrant Descriptions

Leaders

Leaders provide products that are a strong functional match for the market's general requirements. These vendors have been the most successful at building an installed base and revenue stream in the SIEM market. In addition to providing technology that is a good match for current customer requirements, Leaders show the ability to meet the market's future requirements, in most cases, requirements. They typically have a relatively high market share and strong revenue growth, and receive positive customer feedback about their SIEM capabilities and related service and support.

Challengers

Challengers have multiple product and/or service lines, at least a moderately sound SIEM customer base, and sufficient resources to sustain their market presence. Their ability to execute is hindered by strong execution capabilities, as evidenced by financial resources and a significant sales and field presence. However, Challengers either do not demonstrate a complete set of SIEM capabilities or lack a clear vision of the market's direction, or their product functionality does not meet the more stringent requirements.

Visionaries

Visionaries provide products that are a strong functional match for the SIEM market's general requirements, but have less Ability to Execute than Leaders. Their lower Ability to Execute is typically caused by their relatively low market share and revenue, or by their relatively low rate of growth, meaning they expand in a point-in-time analysis by demand for threat management (and accounts) by compliance requirements. Our overall evaluation of vendors in the Magic Quadrant includes an assessment of their ability to meet the market's future requirements, in most cases, requirements to support cloud and regional compliance requirements for data residency and privacy.

Table 3: Completeness of Vision Evaluation Criteria

Image Table ⊡

Evaluation Criteria ↓	Weighting ↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Low
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (October 2022)

Market Overview

The SIEM market grew from $4.01 billion in 2020 to $4.10 billion in 2021 (see Market Share: All Security Software Markets, Worldwide 2021). In 2021, annual growth rate compared to a 11% decline the previous year. Revenue growth, drivers of a SIEM purchase are threat detection, response, compliance, and security operations. Vendors are adding more capabilities to their offerings, including SaaS, to satisfy multiple security and business use cases with capabilities to support a diverse environment.

The SIEM market is maturing at a rapid pace and continues to be extremely competitive. The vendors that sell SIEM solely just from gaps in strategy to detects from other SIEM's are probably today.

SIEM is now and is expected to improve management capabilities by leveraging data points such as configuration status of cloud assets, risk profiling across users and entities, asset inventory and vulnerability data, and threat intelligence. Organizations that have SIEM deployments are looking to leverage their investments and management SIEM leaders built a compelling business case for purchasing based on outcome-delivered metrics (see Tool: Calculating ef Business Aligned Outcome-Driven Metrics for Security Leaders). Security leaders need to identify the business about what data a SIEM will deliver rather than focusing on data that it collects.

The SIEM market has been moving toward a feature-rich security solution to offer clients numerous options to address their security needs, such as:

Threat detection

- Real-time analytics
- Batch analytics
- Data science algorithms
- User and entity-based analytics

Response

- SOAR
- Incident management
- Collaboration

Exposure management

- Asset details (ownership, geography, location, patch status, etc.)
- Cost details (criticality, peer grouping, business unit, risk, incident history, etc.)
- Configuration posture (cloud-native configurations, GPO settings, etc.)
- Poly-cloud visibility and unified exposure understanding
- Threat detection framework alignment

Compliance

- Reporting
- Continuous monitoring requirements
- Audits
- Security system of record

The most prominent deployment architectures that protect from client-hosted and managed, to cloud native (SaaS) or cloud-delivered (hosted) to data storage of cloud deployments, scalability and flexibility. SaaS options reduce buyer requirements to manage and maintain a SIEM deployment. Vendors have made it easier for customers to deploy and maintain SIEM technology by using cloud software services. This shift to SaaS has created a competitive landscape in which vendors have convey of their security tools, and the current market growth supports this. In turn, we have seen a significant increase in the number of SIEM vendors. Organizations are looking for the optimization of current SIEM solutions. There are markets where organizations have multiple architectures remain a requirement (for most, and SIEM vendors need to continue to expand support in cloud platforms, such as Microsoft Azure, Amazon Web Services, and Google Cloud Platform, and vendors will access, which SIEM vendors will address by deploying their solutions regionally, and restrict data residency based on buyer requirements.

The SIEM market will continue to evolve and see increased competition with new solutions that have come to market. Extended detection and response (XDR) is targeted at organizations with a less-mature security operations capability, and it is a SaaS-based, cloud-native solution. Many XDR buyers are prone to buying vendor-delivered service wrapped in SIEM. Organizations that are looking for a choice to run the security solution they have purchased due to lack of resources.

SIEM vendors have begun to invest in or acquire internally collective solutions to deliver a product ecosystem of security technologies for buyers who are looking for an encapsulated security solution. The SIEM market is consolidating around vendors that have demonstrated a strong ability to execute and strategy, and organizations are looking for a single vendor to provide a security solution. Vendors that have a compelling business case for purchasing based on outcome-delivered metrics (see Tool: Calculating ef Business Aligned Outcome-Driven Metrics for Security Leaders). Security leaders need to identify the business about what data a SIEM will deliver rather than focusing on data that it collects.

The SIEM market has been moving toward a feature-rich security solution to offer clients numerous options to address their security needs, such as:

Threat detection

- Real-time analytics
- Batch analytics
- Data science algorithms
- User and entity-based analytics

Response

- SOAR
- Incident management
- Collaboration

Exposure management

- Asset details (ownership, geography, location, patch status, etc.)
- Cost details (criticality, peer grouping, business unit, risk, incident history, etc.)
- Configuration posture (cloud-native configurations, GPO settings, etc.)
- Poly-cloud visibility and unified exposure understanding
- Threat detection framework alignment

Compliance

- Reporting
- Continuous monitoring requirements
- Audits
- Security system of record

The most prominent deployment architectures that protect from client-hosted and managed, to cloud native (SaaS) or cloud-delivered (hosted) to data storage of cloud deployments, scalability and flexibility. SaaS options reduce buyer requirements to manage and maintain a SIEM deployment. Vendors have made it easier for customers to deploy and maintain SIEM technology by using cloud software services. This shift to SaaS has created a competitive landscape in which vendors have convey of their security tools, and the current market growth supports this. In turn, we have seen a significant increase in the number of SIEM vendors. Organizations are looking for the optimization of current SIEM solutions. There are markets where organizations have multiple architectures remain a requirement (for most, and SIEM vendors need to continue to expand support in cloud platforms, such as Microsoft Azure, Amazon Web Services, and Google Cloud Platform, and vendors will access, which SIEM vendors will address by deploying their solutions regionally, and restrict data residency based on buyer requirements.

The SIEM market will continue to evolve and see increased competition with new solutions that have come to market. Extended detection and response (XDR) is targeted at organizations with a less-mature security operations capability, and it is a SaaS-based, cloud-native solution. Many XDR buyers are prone to buying vendor-delivered service wrapped in SIEM. Organizations that are looking for a choice to run the security solution they have purchased due to lack of resources.

SIEM vendors have begun to invest in or acquire internally collective solutions to deliver a product ecosystem of security technologies for buyers who are looking for an encapsulated security solution. The SIEM market is consolidating around vendors that have demonstrated a strong ability to execute and strategy, and organizations are looking for a single vendor to provide a security solution. Vendors that have a compelling business case for purchasing based on outcome-delivered metrics (see Tool: Calculating ef Business Aligned Outcome-Driven Metrics for Security Leaders). Security leaders need to identify the business about what data a SIEM will deliver rather than focusing on data that it collects.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for this defined market. This includes current product capabilities, messaging, service, and teams that provide these products and services, including administration and performance as defined by the market definition and description in "Definition."

Overall Viability: 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 presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors react, 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 "brand image" can be driven by a combination of publicity, promotional initiatives, thought leadership, organic and paid content, social media, and blogs.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. This could include, but is not limited to, ancillary tools, customer support, access to expert, customer communities, quality of relationships, service delivery, and 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 differentiators/functionality, methodology and feature sets as they relate 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 preemptive 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.

© 2022 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The value and quality of research publications vary by author. The views of Gartner's research organization may be influenced by business relationships with vendors. Gartner does not endorse any company or vendor. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may address legal and financial issues, Gartner does not provide legal or tax advice. The opinions expressed herein are subject to change without notice. Gartner's research products are provided on an "as-is" basis and are of little utilization or accuracy. Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without any influence or bias. For more information, see "Guiding Principles on Independence and Objectivity."