Gartner. Licensed for Distribution

Magic Quadrant for Security Information and Event Management

Published 29 June 2021 - ID G00467384 - 58 min read

By Kelly Kavanagh, Toby Bussa, and 1 more

Security and risk management leaders increasingly want SIEM solutions with attack detection, investigation, response and compliance capabilities, but must balance this desire with an understanding of the resources needed to run such solutions. This report will help them identify a suitable vendor.

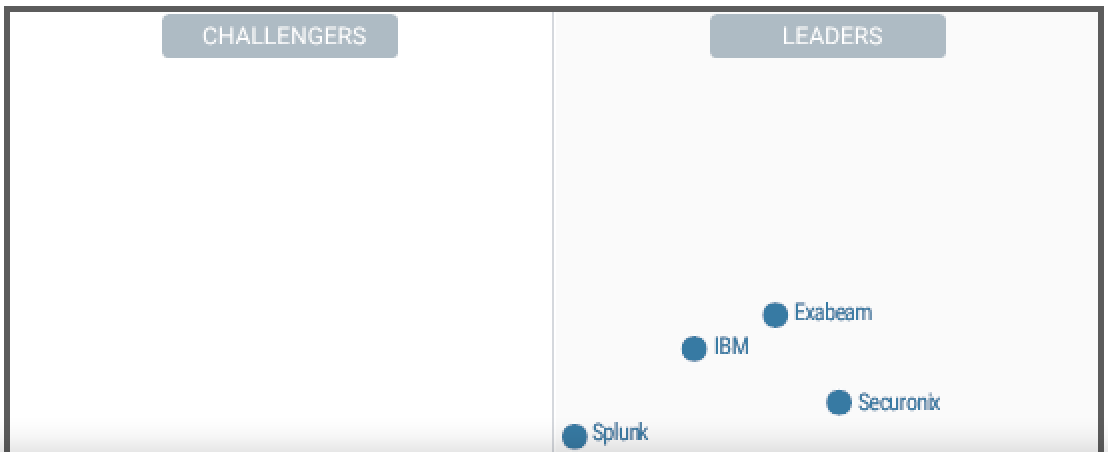
Market Definition/Description

Gartner's view of the market for security information and event management (SIEM) solutions focuses on transformational technologies and approaches to meeting the future needs of end users. It does not focus on the market as it is today.

purposes of scoring, prioritization and expediting investigations. The data should ideally be normalized, so that events, data and contextual information from disparate sources can be analyzed more efficiently for specific purposes, such as network security event monitoring, user activity monitoring and compliance reporting. The technology offers real-time analysis of events for security monitoring, advanced analysis of user and entity behaviors, querying and long-range analytics for historical analysis, other support for incident investigation and management, and reporting (for compliance requirements, for example).

Magic Quadrant

Figure 1: Magic Quadrant for Security Information and Event Management



Elastic

Elastic is a Niche Player in this Magic Quadrant. Elastic is based in Mountain View, California, U.S., the Netherlands and Singapore. It has customers worldwide. Its SIEM platform is Elastic Security, which offers endpoint security, following Elastic's acquisition of Endgame in 2019. Its customers include midsize organizations but mainly large enterprises. Elastic's SIEM platform became generally available in February 2020. Elastic Security can be deployed on-premises or consumed as SaaS via Elastic Cloud. Elastic has a subscription model featuring Standard (formerly Basic) and Premium tiers (Gold, Platinum and Enterprise), available as self-managed software and via Elastic Cloud. The company's resource-based pricing model is based on the memory resources used to store, search and analyze data.

Strengths

- **Opportunity to start for free and grow into advanced offerings:** Elastic has a history of being used for SIEM use cases through the Elasticsearch, Logstash and Kibana (ELK) Stack. Buyers considering Elastic Security can use the free version under the Standard subscription tier, which includes core SIEM functions. Buyers looking for advanced SIEM features and functionality can subscribe to the Gold, Platinum or Enterprise tiers.

- **Variety of sources for detection content:** Elastic provides Elastic Security buyers with its own out-of-the-box detection content, but content is also available from other sources, such as the Elastic user community and SOC Prime.

- **Support for threat-hunting activities:** Elastic's Kibana Lens feature enables a business intelligence some functions can be managed only via developer tools within Kibana, while others are managed via a task-specific GUI.

Exabeam

Exabeam is a Leader in this Magic Quadrant. Its headquarters are in Foster City, California, U.S., and it has offices worldwide. The majority of its customers are in North America, with the next-largest concentrations being in Europe, Asia/Pacific and Latin America. Most customers are large enterprises, but there are also some midsize clients. Exabeam's SIEM solution is available on-premises, as SaaS (Exabeam Fusion SIEM [formerly SaaS Cloud]) and for hybrid, federated deployment. It includes Exabeam Data Lake, Advanced Analytics, Threat Hunter, Entity Analytics, Case Manager and Incident Responder. These components can be bundled or acquired separately to augment an existing SIEM product. Add-ons include Exabeam Cloud Connectors and Cloud Archive. Licensing is term-based. Pricing is normally based on the number of users or entities monitored, but there is also optional data volume pricing for SaaS.

Strengths

- **Long-term, searchable log storage:** The combination of Exabeam Cloud Archive (for up to 10-year data retention), search across normalized events, anomalies, indicators of compromise, and a timeline of log events with automated enrichment enables hunting and investigation supported by rich context over long time frames.

- **Modular architecture for tailored deployment:** Exabeam's modular architecture enables customers

- **Product ecosystem:** Exabeam has no add-on products for advanced endpoint or network detection, but relies on integrations with leading third-party products or open-source solutions. Several competing SIEM vendors offer their own technology, in addition to supporting third-party products.

FireEye

FireEye is a Niche Player in this Magic Quadrant. Its headquarters are in Milpitas, California, U.S. Most of its customers are in North America, with the next-largest concentrations being in Europe, the Middle East and Asia. FireEye provides a number of security detection offerings to complement its FireEye Helix extended detection and response (XDR) platform, including network, email, file analysis, packet capture, endpoint, threat intelligence and managed service offerings. FireEye Security Orchestrator provides security orchestration, automation and response (SOAR) capability, for no additional license cost. Helix is a cloud-based SaaS-only SIEM solution, for which pricing is based on events per second (EPS) for data ingestion.

Strengths

- **Ecosystem of threat-centric solutions:** FireEye's ecosystem offers threat-centric solutions for hosts, networks and the cloud that are integrated with, and complementary to, Helix. There is also an option to overlay 24/7 security operations center (SOC) services from Mandiant Managed Defense. This single ecosystem approach will appeal to buyers looking for a single-vendor sourcing option.

Fortinet

Fortinet is a Visionary in this Magic Quadrant. Fortinet is headquartered in Sunnyvale, California, U.S. It has a global footprint and customers in all major world regions, but especially North America and Europe. Its SIEM solution is FortiSIEM. This product includes Advanced Agents (for Windows-based user and entity behavior analytics [UEBA] capabilities). FortiSIEM integrates with FortiSOAR, FortiAnalyzer and other elements of Fortinet's security product suite. Pricing is based on devices, EPS and number of agents. FortiSIEM is available as a virtual or physical appliance. Perpetual and subscription licenses are available.

Strengths

- **Support for service providers and complex organizations:** Fortinet FortiSIEM offers built-in multitenancy support for complex organizations and service providers, as well as a variety of features specific to them. It also offers a consumption-based model for managed security service providers (MSSPs) with unlimited EPS.

- **Native asset visibility capabilities:** Fortinet FortiSIEM has powerful asset discovery capabilities and a built-in configuration management database (CMDB). The CMDB provides centralized visibility of assets discovered via active scanning and passive log inspection.

- **Integration of FortiSIEM with the wider Fortinet ecosystem:** Fortinet offers a diverse ecosystem of security and network products integrated via the Fortinet Security Fabric. Prospective customers and existing Fortinet clients looking for a single vendor to provide them with threat-monitoring, detection and response solutions should consider Fortinet.

Gurucul is a Visionary in this Magic Quadrant. Gurucul is headquartered in Los Angeles, California, U.S. Its largest concentration of customers is in North America, with the next-largest concentrations being in Europe, Asia, the Middle East and Latin America. Its SIEM solution, Gurucul SIEM, is part of the Gurucul Risk Analytics platform. It is available as SaaS, and for on-premises or hybrid deployment. Components include Log Aggregator, Threat Hunting, Security Data Lake, a Network Traffic Analysis engine, SOAR, as well as Identity Analytics and User & Entity Behavior Analytics. Gurucul offers perpetual and subscription licenses, which can be monthly, annual or multiyear. Pricing is based on the number of users and entities monitored.

Strengths

- **User and identity monitoring capabilities:** When the premium Identity Analytics module is licensed, this extends the applicability of Gurucul's solution from SecOps to identity and access management (IAM) and privileged access management (PAM) teams.
- **Variety of deployment options:** Gurucul offers cloud-based, on-premises and "do it yourself" CIPS options, hybrid (cloud and on-premises) deployment, and integration with a customer's existing Hadoop-powered data lake. Supported formats include software, containerized, physical appliance, virtual appliance and cloud-based single/shared-tenant. Gurucul supports parent-child deployment options.
- **Gurucul STUDIO:** This component provides a comprehensive analytics builder and rule customization interface for beginners and advanced security analysts alike. Any of the provided data-science-based analytics tools can be customized. Alternatively, users can build their own

Huawei is a Niche Player in this Magic Quadrant. Huawei has headquarters in Shenzhen, China. Its SIEM customers are largely concentrated in China; others are in the Middle East, Africa and Latin America. Its SIEM solution is called HiSec Insight, and there are numerous additional modules and companion technologies for feature- or architecture-specific requirements. Its customer base is split almost evenly between large and midsize enterprises, but there are also some smaller clients. Pricing for on-premises deployments is based on data velocity (EPS) and volume (gigabytes per day), plus log retention and add-on modules. SaaS deployments are based on the number of Elastic Container Services (ECSs) purchased.

Strengths

- **Behavioral analytics:** Analytics has been an area of investment by Huawei. Its user behavior analytics provide dynamic peer-group-based detections. Its ML-based risk ranking for entities reflects factors such as asset value, associated rule-based detections and vulnerability data.

- **Extensive product ecosystem:** Huawei offers a number of integrated capabilities, including network detection and response, sandboxing, deception, user behavior analysis, orchestration and response, and threat intelligence.

- **Flexibility in relation to form factors:** Huawei's product is available in multiple form factors that can be mixed as needed. These include software, physical and virtual appliances. There are also options for hosting on Huawei's public or private cloud infrastructure.

Cautions

unlimited capacity for on-premises deployments only (perpetual or subscription license). Capacity-based (EPS) licensing is available for on-premises and SaaS deployments (QRadar on Cloud [QROC]).

Strengths

- **Ability to event filter at the collection layer:** IBM QRadar can remove undesired data before it is forwarded for correlation and storage. This gives users the ability to fine tune their security-relevant data sources to reduce EPS costs, and use lower-cost native log management for data that is less relevant to security use cases.

- **Simplified deployment and management of analytics:** IBM's QRadar Use Case Manager (UCM) enables a user to search and filter for any analytic condition, and turn on or off, edit, copy and visualize analytic dependencies. UCM also extends to MITRE ATT&CK coverage and presents required data source types for tactics, techniques and procedures (TTP) detection.

- **Support for Purdue Model Levels 2 (and above) in operational technology and industrial control system environments:** IBM QRadar offers this using the Disconnected Log Collector (DLC) as a data diode that prevents bidirectional access. Flow collectors can monitor network traffic in passive mode.

Cautions

- **Transition of product lines:** IBM is in the process of integrating QRadar functionality into its Cloud Pak for Security platform in order to modernize its capabilities and end-user experiences. Big is available only as SaaS. LogPoint acquired agileSI in August 2020 to bolster its SAP security capabilities.

Strengths

- **Marketing and products aligned with specific use cases:** LogPoint markets product-specific capabilities, such as SAP security monitoring and Evaluation Assurance Level (EAL) 3+ certification, to relevant organizations (such as those using SAP ERP) and sectors like government and manufacturing.
- **Support for service providers and complex organizations:** LogPoint has native multitenant capabilities. Additionally, the LogPoint Director solution add-on supports central management of multi-instance deployments, which will appeal to service providers and organizations looking for a SIEM solution that can support a parent-child deployment model (for example, those with a headquarters that supports various lines of business).
- **Native data privacy and protection features:** Capabilities such as data masking and obfuscation help address privacy and data protection requirements related to the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Cautions

- **Footprint outside Europe:** Europe is both LogPoint's home market and its largest market. LogPoint lags behind many competitors in terms of direct sales in other regions. LogPoint indicates, the rest in Asia/Pacific, the Middle East and Africa, and Latin America. Its customer base is skewed toward midsize enterprises and smaller organizations, though large enterprises have also purchased its platform. There is a cloud-hosted deployment option, but most customers deploy its platform on-premises. Licensing is available on a perpetual basis (priced by average number of messages per second per day) or a subscription basis (priced by number of employees).

Strengths

- **Extensive resellers:** LogRhythm has a strong team of reseller partners in every major world region. This strength is mirrored by broad support from managed service providers to help modestly resourced buyers manage and monitor its SIEM platform.
- **Pilot and proof of concept (POC) options:** Buyers can take advantage of several types of pilot and POC program, ranging from prepilot workshops to hosted, scenario-based test-drive exercises and "try and buy" options.
- **Investigation and case management workflow:** LogRhythm provides mature and refined investigation and case management capabilities that assemble context and enable users to create an evidence base for case disposition.

Cautions

- **Limited cloud-based options:** LogRhythm's recent acquisitions and product roadmap demonstrate progress in preparing to offer cloud-native SIEM capabilities, but the vendor lags behind many perpetual basis. Pricing for SaaS deployment is based on the amount of data stored in the cloud over a specific period, whereas on-premises pricing is based on the number of event sources or assets.

Strengths

- **Out-of-the-box incident response playbooks and workflows:** ManageEngine's Log360 solution provides many of these, with features that allow for custom content creation. For organizations with an existing incident or case management system, Log360 integrates with popular ticketing and incident management platforms.
- **Reporting engine:** ManageEngine's reporting engine is comprehensive, with support for numerous compliance-framework-focused outputs and alerting based on compliance violations.
- **Product support:** Reviewers on Gartner's Peer Insights platform have praised ManageEngine's support for the Log360 product.

Cautions

- **Use-case support:** There is a noticeable lack of support in ManageEngine's Log360 solution for, among other things, cloud services, applications and operational technology, industrial control systems, and Internet of Things (IoT) asset monitoring.
- **Support for third-party solutions:** Third-party collaboration products, external SOAR, UEBA, endpoint security and NDR technologies are notably absent from the list of technologies supported by ManageEngine Log360.

- **Support for compliance use cases and requirements:** Buyers that need coverage for a range of compliance regulations and standards around the world will be well supported by McAfee ESM.
- **Ability to consolidate SIEM and other solutions:** Buyers who want a SIEM product and to standardize on a single vendor's product ecosystem should consider McAfee. It offers a range of complementary solutions, such as an endpoint detection and response (EDR) solution, a CASB, an intrusion prevention system and a secure web gateway.

Cautions

- **Limited advanced features and add-ons:** McAfee lags behind competing SIEM vendors that offer cloud-native SIEM options, ML-powered UEBA and SOAR add-on solutions.
- **Requirement for add-ons for a range of cloud environments:** Native monitoring of popular SaaS solutions and CIPS by McAfee ESM is limited to Microsoft Office 365, AWS and Microsoft Azure. Other SaaS apps and CIPS require use of MVISION Cloud or an integration with a third-party CASB.
- **Potential impact from sale of enterprise business:** In March 2021, McAfee announced the sale of its enterprise business to Symphony Technology Group. This sale may introduce uncertainty for existing customers and potential buyers. Those considering McAfee for SIEM should check its roadmap and future support for McAfee ESM.

Micro Focus

- **MITRE ATT&CK mapping:** Micro Focus' platform offers extensive mapping of detection content to the MITRE ATT&CK framework.

Cautions

- **Lack of consistency in deployment options:** Work on Micro Focus' ArcSight architecture is in progress, and this may complicate selection, deployment and management of its solution. Although components are available as software images, support for deployment in other formats differs. Some components are available as physical appliances. Some are available in a containerized framework. Some are available with support for cloud-native services in select clouds.
- **Limited cloud and SaaS coverage:** Micro Focus' out-of-the-box monitoring capabilities for SaaS and cloud infrastructure are more limited than those of many competitors. Although Microsoft Office 365 applications are supported, several other popular SaaS business applications, including those of Salesforce and Workday, require connector customization. AWS CloudTrail and other services are supported, as are several Microsoft Azure services, but other cloud platforms require connector customization.
- **POC and pilot support:** Micro Focus has no formalized and generally available POC or pilot program. POC requests are addressed on a case-by-case basis, with the exception that CrowdStrike customers can request a POC for the SaaS UEBA capability via the CrowdStrike market. By contrast, several SIEM competitors have extensive and easy-to-access POC and pilot

whereby customers can consume as in a pay-as-you-go model or buy a set amount of reserved capacity.

- **Breadth and scope of product portfolio:** Microsoft offers a rich ecosystem of security and other IT solutions (Microsoft 365 Defender, Azure Defender, Office 365 and Azure) that are natively integrated with Azure Sentinel. This will appeal to customers who have invested in these Microsoft solutions.

- **Integration capabilities:** Azure Sentinel has a robust API interface that allows for flexible interfaces, based on a user's needs and requirements. This will appeal to organizations that want to interface with Azure Sentinel using different methods, not just via the Azure Sentinel workspace interface (like MSSPs).

Cautions

- **Lack of SIEM functionality in some areas:** Azure Sentinel customers will find that functions that are native to many vendors' SIEM offerings, such as connectivity to ITSM solutions, require the use of Azure Logic Apps, another piece of the Azure ecosystem. Additionally, out-of-the-box compliance reporting for common requirements and standards is limited. Azure Security Center provides coverage for CIPS-related compliance with ISO 27001, PCI Data Security Standard (DSS) and Azure CIS. Watchlists are a preview feature at the time of writing.

- **Need for familiarity with Azure ecosystem:** Users need some familiarity with the Azure ecosystem, During the past 12 months, NetWitness was sold and spun out of Dell Technologies as a stand-alone business within RSA.

Strengths

- **Support for security operations centers (SOCs) wanting a single-vendor ecosystem:** NetWitness' NWP is a comprehensive platform that will appeal to SOCs that want a single vendor for modern SOC instrumentation, including integrated SIEM, UEBA, SOAR, EDR, network threat analytics (NTA, including packet capture), and IoT monitoring technologies.

- **Hybrid deployment options:** For organizations looking for an on-premises or hybrid model with their private clouds or public CIPS, the NWP is highly flexible in terms of where and how components can be deployed. Licensing of NetWitness Logs is based on data consumption, not product components (such as decoders, log collectors, concentrators and brokers), so as many components as are required can be utilized without increasing the license cost.

- **Support options:** NetWitness offers a variety of training options through the RSA University — remote, self-paced and in-person. An on-demand subscription is also available for access to training when needed.

Cautions

- **Limited SaaS option:** NetWitness' options for cloud SIEM are limited to Orchestrator (SOAR), IoT monitoring and the Detect AI product. Buyers have to handle their own deployments of other NetWitness components in their own private clouds or CIPS. Alternatively, they can choose a including EDR and security services. Its SIEM product is ClearSkies SaaS NG SIEM. Related solutions (or available modules) include the Identity and Access Service module, ClearSkies NG Endpoint Detection & Response (EDR), and ClearSkies NG Active Defense. ClearSkies is available as SaaS only, and the licensing model is subscription-based. Pricing is based on data volume (gigabytes) per day.

Strengths

- **Simplicity of product licensing:** Odyssey's SIEM product is licensed by volume (gigabytes per day) as a subscription, which is simple. Options for three-, six- and 12-month licenses are available. Each period offers a fixed amount of data, an analysis window (in weeks), support for a certain number of users and storage. Additional options are available in the same subscription windows and are priced accordingly (for example, per EDR agent, portal user, deception decoy or beacon trap).

- **Potential for integration with EDR solution:** Odyssey has its own EDR solution, which can be integrated with its ClearSkies SIEM solution.

- **Optional deception add-on:** Odyssey offers Active Defense as an optional deception add-on, which is unusual in the SIEM sector.

Cautions

- **Concentration on southern Europe and the Middle East and Africa:** Odyssey has only a very small number of clients in the Americas and Asia/Pacific.

- **One platform with multiple security products:** Rapid7's core SIEM platform offers logging and threat detection, including UEBA, via endpoint agents, and deception technology, along with incident management and reporting. Optional add-ons from Rapid7 offer vulnerability management, network monitoring, orchestration and response, and cloud security posture management.

- **Curated experience for modestly resourced customers:** Rapid7 manages detection content and threat intelligence feeds on the Insight platform, thus minimizing the need for customers to do so.

- **Managed detection and response service:** This is available from Rapid7, at additional cost. It represents a single source for customers that want access to the SIEM product and need service support for monitoring and investigation.

Cautions

- **Compliance:** Rapid7's out-of-the-box support for regulatory compliance reporting formats is limited to PCI DSS and the U.S. Health Insurance Portability and Accountability Act (HIPAA). Customers with other requirements need to create dashboards and reports.

- **Geographic availability:** InsightIDR is hosted on AWS. Buyers who need their data to reside in specific geographies should confirm that Rapid7 enables this. At the time of writing, InsightIDR is not available in South America or the Middle East.

- **Customization:** Buyers with requirements for extensive development of detections and analytics

- **Managed service partner support:** Securonix has secured partnerships with numerous large managed service partners over the past 18 months. These enable midsize and smaller organizations to use its product with the support of expert services.

- **Threat intelligence support:** Securonix provides extensive threat intelligence platform (TIP) capabilities natively. It also provides out-of-the-box integrations with a broad range of third-party TIP products.

Cautions

- **Platform management on-premises:** End-user customers using Securonix SIEM solution on-premises have reported that deploying and managing it have proved complex and challenging undertakings. They recommend seeking training and assistance from professional services.

- **Product support:** Users have reported lower levels of satisfaction in several product support areas than is the case for many of Securonix's competitors for on-premises deployments. Securonix has hired senior leaders in engineering, customer success and operations to drive service improvement.

- **On-premises scalability:** Prospective buyers should check Securonix's ability to meet workload requirements for large-scale on-premises deployments.

Splunk

for Splunk Cloud), in addition to tiered pricing models available to non-public-sector buyers (Predictable Pricing). Buyers now have different options available, the better to align their Splunk usage with different pricing models.

- **Visibility with buyers:** Splunk maintains a high level of visibility to SIEM buyers in North America and Europe. It is less visible to buyers in Asia/Pacific, Latin America and the Middle East.

Cautions

- **Price and contract flexibility:** Feedback from Gartner clients indicates concerns about the cost of Splunk. Reviewers on Gartner's Peer Insights platform have tended to give Splunk lower scores for pricing and contract flexibility than those received by many competitors.
- **Lack of fully cloud-native security operations suite:** Splunk Enterprise Security is offered in Splunk Cloud, but buyers wanting an entirely cloud-delivered option that includes Splunk UBA and Phantom must deploy those solutions in their own CIPS, or ask Splunk whether hosted options are available in their geographies. Mission Control can help minimize the impact by providing a single UI for all three solutions, regardless of where they are deployed.
- **Geographic support for Splunk Cloud:** Buyers in North America, Europe and Asia/Pacific are supported by appropriate points of presence for Splunk Cloud. But buyers in the Middle East, Africa and Latin America will need to check whether they can be supported, if they have concerns about, or requirements for, data residency.

improved performance of the solution over time. Other user-facing solutions provide threat analytics and recommendations based on cross-customer analysis of specific data sources and threat feeds.

- **Robust event filtering, masking and routing:** Sumo Logic's event collector supports extensive filtering to manage ingestion, masking and hashing in order to help meet data privacy needs. It also supports flexible routing and bandwidth management for low-bandwidth environments.

Cautions

- **Analytics coverage:** Sumo Logic's out-of-the-box security detection capabilities are not as extensive as those available in other vendors' SIEM products. Advanced analytics for user behavior are not as mature as those of several SIEM competitors.
- **Resource estimation:** Sumo Logic's credit-based model may challenge buyers who lack experience with estimating the ingestion volume and investigation resources needed to meet their requirements. Buyers should establish processes to monitor credit usage and budgets to avoid license capacity issues.
- **Uneven support for integrations:** Although users can install and run most apps from Sumo Logic's application library, an app for PCI compliance and another for security analytics require enterprise licensing and a paid professional services contract to install and configure.

- **Comprehensive custom rule creation features (including condition trees and graphical views):** Rules can be nested for complex correlation, and include thresholds, counts and actions to take. Intelligence enrichment can be configured in a similar way to a TIP solution.

Cautions

- **Support for customers outside China with compliance requirements:** Venustech's SIEM product provides a compliance package for Chinese customers, but at extra licensing cost. Prospective buyers elsewhere should check whether Venustech can support their regulatory compliance requirements.

- **Support for SaaS apps outside China:** Venustech does not support SaaS apps beyond China, and its CIPS support is limited to Alibaba, Tencent, Huawei and Inspur.

- **Support for third-party solution investments:** Venustech's product may not support, for example, machine-readable threat intelligence solutions. SOAR integration is limited to its own solutions.

Vendors Added and Dropped

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 be a reflection of a change in the market and,

- HanSight, which did not meet the commercial requirements for inclusion in this Magic Quadrant.
- SolarWinds, which did not meet the analytics-related requirements for inclusion in this Magic Quadrant.

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:

- The vendor's product had to provide security information management (SIM) and security event management (SEM) capabilities to end-user customers via software and/or appliance and/or SaaS.
- The vendor's SIEM product had to provide a range of detection analytics, from basic correlation though advanced analytics (such as machine learning for UEBA), via native capabilities or via tight integration with an add-on product sold by the SIEM vendor.
- SIEM features, functionality and add-on solutions had to be generally available as of 1 November 2020.

- The vendor had to have sales and marketing operations (via in-region sales offices or named in-region resellers) targeting at least two of the following regions as of 30 September 2020: North America, EMEA, Asia/Pacific, Latin America.

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, or managed SIEM, or other managed services offering. By managed services, we mean those in which the customer engages the vendor to establish, monitor, escalate and/or respond to alerts, incidents and cases.

Honorable Mentions

- **AT&T Cybersecurity:** This vendor's USM Anywhere offering is being repositioned as a service delivery platform, rather than a SIEM offering.
- **Devo:** This vendor did not meet the functional or commercial requirements for inclusion in this Magic Quadrant.
- **Graylog:** This vendor did not meet the functional requirements for inclusion in this Magic Quadrant.

Overall Viability: This criterion includes an assessment of a vendor's financial health, the financial and practical success of its overall company, and the likelihood that it will continue to invest in SIEM 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 base, growth rates for its SIEM revenue and installed base, its presales support, and the overall effectiveness of its sales channel. The level of interest from Gartner clients is also considered.

Market Responsiveness/Record: This criterion evaluates how well matched a vendor's SIEM offering is to the functional requirements expressed by buyers at the time of acquisition, and the vendor's track record of delivering new functions when they are needed by the market. Also considered is how the vendor differentiates its offerings from those of its major competitors.

Marketing Execution: This criterion evaluates a vendor's SIEM marketing messages in light of Gartner's understanding of customers' needs. It also evaluates any variations by industry or geographic segment.

Customer Experience: This criterion evaluates product function and service experience in production environments. Included are ease of deployment, operation, administration, stability, scalability and vendor support capabilities. This criterion is assessed on the basis of analysis of feedback received via Gartner's client inquiry service, reviews on Gartner's Peer Insights forum, and other interactions with Gartner clients that are using, or have completed competitive evaluations of, a vendor's SIEM

Evaluation Criteria	***Weighting***
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	Medium
Operations	Medium

Source: Gartner (June 2021)

Completeness of Vision

Market Understanding: This criterion evaluates a vendor's ability to understand buyers' current and emerging needs, and to translate that understanding into products and services. SIEM vendors that attribute over breadth of coverage beyond basic use cases. SIEM products are complex and tend to become more so as vendors extend their capabilities. Vendors able to provide effective products that users can successfully use as a service, or deploy, configure and manage with limited resources, will be the most successful.

We evaluate options for co-managed or hybrid deployments of SIEM technology and supporting services, because growing numbers of Gartner clients are anticipating or requesting ongoing service support for monitoring or managing their SIEM technology deployments.

Vertical/Industry Strategy: This criterion evaluates a vendor's strategy to support SIEM requirements specific to industries.

Innovation: This criterion evaluates a vendor's development and delivery of SIEM technology that is differentiated from that of its competitors in a way that uniquely meets customers' most important requirements. Product capabilities and customer use in areas such as application layer monitoring, identity-oriented monitoring and incident investigation are evaluated, in addition to other product-specific capabilities that are needed and deployed by customers. Heavy weightings are assigned to capabilities needed for advanced threat detection and incident response: user, data and application monitoring; ad hoc queries; visualization; orchestration and incorporation of context to investigate incidents; and workflow/case management features.

Geographic Strategy: This criterion takes account of the fact that, although the North American and EMEA markets produce the most SIEM revenue, Latin America and Asia/Pacific are growth markets

Evaluation Criteria	*Weighting*
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	Medium

Source: Gartner (June 2021)

Quadrant Descriptions

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 due to lower scores for product features and functions, or to a smaller presence in the SIEM market than that of the Leaders, as measured by installed base, revenue size or growth, overall company size or general viability (or a combination of these attributes).

Niche Players

Niche Players are primarily vendors that provide SIEM technology that is a good match for a specific SIEM use case or a subset of the SIEM market's functional requirements. Niche Players focus on a particular segment of the client base (such as midsize organizations, service providers, or a specific region or industry) or may provide a limited set of SIEM capabilities. In addition, Niche Players may have a small installed base or be limited, according to Gartner's criteria, by other factors. These factors may include limited investments or capabilities, a geographically limited footprint, or other inhibitors to providing a broad set of capabilities to organizations now and during a 12-month planning period. Inclusion in this quadrant does not reflect negatively on a vendor's value for narrowly focused markets or use cases.

Context

SIEM technologies provide core SIM and SEM functions, along with a variety of advanced features and complementary solutions and capabilities. They support near-real-time security event monitoring, threat detection (both in real time and via historical analysis), incident investigation and response, and compliance requirements. Core functions include:

- Monitor the activities of users and specific types of users, such as those with privileged access (both internal and third parties), and users with access to critical data assets (such as intellectual property), and executives.
- Monitor server and database resource access, and offer some data exfiltration monitoring capabilities
- Support compliance requirements and provide compliance reporting.
- Provide analytics and workflow to support incident response, hunt for threats, and, increasingly, orchestrate and automate actions and workflows, thus powering SOC-type use cases.

SIEM technology aggregates and analyzes the event data produced by networks, devices, systems and applications. The primary data source has been time-series-based log data, but SIEM technology is evolving to process (e.g., for real-time monitoring) and leverage (e.g., for incident investigation and response) other forms of data to obtain context about users, IT assets, data, applications, threats and vulnerabilities (e.g., Active Directory [AD], configuration management database [CMDB], vulnerability management data, HR information and threat intelligence).

Market Overview

The SIEM market grew from $3.55 billion in 2019 to $3.58 billion in 2020 (see Market Share: All Software Markets, Worldwide, 2020). Threat management (and specifically threat detection and use cases based on behavior. Customers are also adding monitoring of IaaS environments and workloads, and SaaS applications, to the scope of monitoring required for SIEM deployments.

SIEM deployments tend to grow in scope over a three-year period to include more use cases and more event sources, and more integrations with complementary technologies such as EDR, NDR and SOAR. However, as organizations reconcile themselves to more distributed workforces and the demand to respond to threats faster, some solutions, like SOAR and EDR, may, in combination with a SIEM product, become parts of an initial deployment. Additionally, as the number of use cases increases, and as they become more complex, there is typically greater demand for resources to run, tune and operate SIEM products, and to respond to incidents.

SIEM Vendor Landscape

Although the SIEM technology market has many mature vendors, there continues to be an influx of new vendors aiming to compete against them. The vendor landscape for SIEM therefore remains dynamic, with established providers and recent entrants delivering cloud-based SaaS offerings, and adding or expanding advanced analytic techniques to help identify and prioritize threats. SIEM vendors continue to improve their investigation and response capabilities through native features and integrations with third-party SOAR solutions.

The SIEM market is characterized by a small number of vendors with large customer bases, and others with smaller, but rapidly increasing customer bases. Splunk, Micro Focus, IBM and LogRhythm command a significant share of the market's revenue. Elastic, Sumo Logic and Gurucul have technology platform, because the vendors provide that support. However, customers must still provide their own resources (or use other service providers) to configure content and monitor and investigate events raised by the SIEM solution. A few SIEM vendors offer managed services delivered by their own staff, so customers can acquire the technology and services from a single vendor. MSSPs, which offer real-time monitoring and analysis of events, and collect logs for reporting and investigation, are another option for SIEM users. Customer-specific requirements for event collection and storage, alerting, investigation, and reporting may prove problematic for external service providers. SIEM users exploring services should evaluate the suitability of providers for current and planned use cases, especially those that include monitoring of SaaS and IaaS.

SIEM Alternatives

The complexity and cost of buying and running SIEM products, and the emergence of other security analytics technologies, has fueled interest in alternative approaches to collecting and analyzing event data to identify and respond to attacks. These alternatives include:

- **Event collection and analytics platforms:** These event collection and analytics products can tackle some SIEM use cases, and possibly other nonsecurity use cases, and may make it easier for buyers to spread the cost across several budgets and develop a broader pool of internal expertise. However, these products may lack support for the full range of capabilities available in a SIEM solution, and may require more user development of detection or investigation content.
- **Extended detection and response products:** These emerging offerings are integrated suites of

Ability to Execute

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

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 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,

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.