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.

Gartner defines this market as catering to customers' need to:

- Collect security event logs and telemetry in real time for threat detection and compliance use cases.
- Analyze telemetry in real time and over time to detect attacks and other activities of interest.
- Investigate incidents to determine their potential severity and impact on a business.
- Report on these activities.
- Store relevant events and logs.

The vendors included in this Magic Quadrant have products designed for this purpose, which they market and sell to the security buying center.

SIEM technology aggregates event data produced by security devices, network infrastructure, systems and applications. The primary data source is log data, but SIEM technology can also process other forms of data, such as network telemetry data (flows and packets). Event data can be combined with contextual information about users, assets, threats, and vulnerabilities for the 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

Source: Gartner (June 2021)

Drag and drop this image to sa

Vendor Strengths and Cautions

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 type of approach to threat-hunting use cases. It combines drag-and-drop visualization capability with the native search capabilities of Elastic's platform.

Cautions

- **Learning curve to understand pricing model:** Elastic's pricing model does not correspond to the market norm of volume-, velocity-, user- or asset-based pricing. A resource-based pricing model may prove complex for some buyers when planning for their initial deployment and future growth. Prospective buyers must ensure they understand the implications of resource-based pricing and how to calculate the required capacity, especially when comparing Elastic's SIEM solution with competing solutions.

- **Lack of out-of-the-box compliance support:** Elastic's platform offers no packaged compliance dashboards and reports. Detection rules relevant to compliance are available, but not tagged or easily identified and deployed. Users must rely on community or partner development, or create their own dashboards.

- **Variable platform management user experience:** The user experience is not fully consistent across Elastic's product when it comes to managing and operating the solution. For example, 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 to select only the capabilities they need for data storage, analytics and response, for example, across multiple hardware, software and cloud form factors. This also enables customers to deploy Exabeam modules to augment a competitor's SIEM deployment.
- **Mature and extensive behavioral analytics:** Exabeam's heritage of machine learning (ML)-driven user and entity behavior detections enables it to cover a broad range of use cases. It offers risk scoring and automated context enrichment for users and entities, along with a timeline for investigation and workflow.

Cautions

- **Regional availability of SaaS:** Exabeam Fusion SIEM, and the Cloud Archive add-on module, which runs on the Google Cloud Platform, are not available uniformly across all regions. Customers in unsupported regions may, however, be able to run Exabeam software in the cloud using bring your own license (BYOL) options in local cloud infrastructure.
- **Sigma support:** In contrast to several competing SIEM vendors, Exabeam offers limited support for Sigma community content. Although some Sigma-generated detections are included in out-of-the-box correlations, other detections and analytics are unique to Exabeam's proprietary data models.
- **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.
- **Provision of network sensors with Helix:** This augments other data and event collection sources with network metadata telemetry for incident investigation and response.
- **13-month default data retention period:** This is a competitive length, as other cloud SIEM products might offer only 30 or 90 days of default storage.

Cautions

- **SaaS-only delivery:** For buyers that require an on-premises option, or that have data sovereignty issues that cannot be addressed by Amazon Web Services (AWS) regions, FireEye Helix may not be a feasible option.
- **Helix analytics:** FireEye lags behind other SIEM vendors in several areas, such as heuristic and behavioral analytics, incident risk scoring, and integration with third-party SOAR solutions. The Helix roadmap indicates plans to address these missing or lacking capabilities, but prospective buyers must monitor the delivery of roadmap items, to ensure FireEye will meet their requirements.
- **No user modification of analytics:** Negating or modifying FireEye analytics can require complex rule creation to achieve the desired outcome.

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.

Cautions

- **Lack of a cloud-delivered option:** FortiSIEM is not available as a SaaS solution. Fortinet relies on partners that offer hosting services for FortiSIEM as a means of delivering a SaaS-like experience to buyers. End users can deploy the solution in their own public or private cloud, or in a hybrid cloud model.
- **Limited coverage for monitoring cloud environments:** FortiSIEM's cloud security coverage is not as strong as that of other competitors. It lacks support for several public cloud infrastructure and platform services (CIPS), and the only cloud access security broker (CASB) supported is Fortinet's own FortiCASB product.
- **User and entity behavior analytics options:** UEBA is available in two flavors: a premium offering and a more limited version native to FortiSIEM. Both require agent deployment, and lack capabilities that are available from competitors, such as the ability to create dynamic peer groups. However, Fortinet's roadmap indicates that these gaps will be addressed.

Gurucul

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 analytics.

Cautions

- **Potentially confusing modularity:** Prospective buyers may struggle to determine what capabilities, features and functionality Gurucul includes in its different packaging options: Unified Security Analytics, SIEM and XDR. For example, although Gurucul’s solution grew out of the UEBA market, the base SIEM license does not include the full range of UEBA capabilities available in the market, to achieve which it requires an add-on module.

- **Limited support for cloud service providers:** Prospective buyers that require cloud deployments in non-Western regions must check whether Gurucul can, or will, support them in monitoring non-Western infrastructure as a service (IaaS) platforms.

- **Limited visibility for SIEM:** Although Gurucul has taken steps to reorient its sales operations and increase its visibility to SIEM buyers, its mind share for SIEM among Gartner clients remains low.

Huawei

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

- **Limited support for cloud infrastructure monitoring:** Monitoring of cloud infrastructures is limited to Huawei's own cloud. None of the other cloud services are supported out of the box.
- **Lack of support for SaaS monitoring:** Out-of-the-box monitoring of popular SaaS applications is not provided. Huawei's platform lacks integrations with Microsoft Office 365, Google Workspace, and applications from Workday, Salesforce and Box.
- **Limited availability:** Huawei's focus on China, emerging markets in Asia/Pacific, and the Middle East and Africa means its product has little exposure to SIEM buyers elsewhere. Nor does Huawei plan immediate expansion to North America and Europe.

IBM

IBM is a Leader in this Magic Quadrant. It is based in Armonk, New York, U.S. IBM's operations focus on North America, Europe, Asia/Pacific, Latin America and the Middle East. IBM Security provides numerous security solutions, in addition to its QRadar SIEM solution, such as Guardium, Trusteer, X-Force Threat Intelligence, Cloud Pak for Security, Verify Access, Privileged Identity Manager, QRadar Network Insights (QNI; for network detection and response [NDR]), WinCollect and QRadar Vulnerability Manager (QVRM; for vulnerability assessment). Licensing is available for server-based, 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 shifts in products are often incremental and may take longer than anticipated to complete.

- **Lack of native collaboration and chat features:** For these, IBM QRadar users have to use third-party solutions or a SOAR add-on. Prospective buyers should check whether their chosen collaboration tools will integrate with QRadar.

- **Potential for complex contracts:** Scoping parameters, deployment models and add-on solutions may result in complex contracts. Pricing can be based on EPS, flows, number of users, number of servers, and number of automated actions, with perpetual and subscription licenses possible in a single proposal. IBM Security customers on Gartner's Peer Insights platform tend to give IBM lower scores for pricing and contract flexibility than those received by many competitors.

LogPoint

LogPoint is in a Niche Player in this Magic Quadrant. LogPoint is headquartered in Copenhagen, Denmark. It has customers worldwide, but with a concentration in Europe. Its SIEM solution offers UEBA and the LogPoint Director (including Director Console and Director Fabric). Complementary solutions include LogPoint for SAP and Applied Analytics. Licensing is by subscription, with pricing based on the number of assets monitored. UEBA is licensed separately, and priced by number of employees and assets. SIEM form factors include physical appliance and software appliance. UEBA 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, however, that it is addressing this issue by investing in, and maturing, its sales operations, as well as by expanding into other regions to complement the activities of its channel partners.

- **Limited form factors:** LogPoint's SIEM solution is available only as an appliance (physical or virtual) — there is no SaaS offering. UEBA is delivered as SaaS, but not available on-premises. Buyers looking for a hosted option need to install LogPoint's solution in their own public or private cloud environment, or use partners that can offer a hosted option. Prospective UEBA buyers should confirm how any data protection and residency requirements can be met.

- **Basic capabilities for incident management and response:** Incident response capabilities, such as case management and support for response actions, are basic. LogPoint lacks a native SOAR option, unlike many competitors, to appeal to buyers that want an integrated SIEM and SOAR solution from the same vendor. LogPoint relies on API integrations with several popular IT service management (ITSM) and SOAR solutions.

LogRhythm

LogRhythm is a Leader in this Magic Quadrant. Its headquarters are in Boulder, Colorado, U.S. Its SIEM platform includes several add-on components to deliver endpoint, network and user behavior analytics capabilities. A large majority of its SIEM customers are in North America and Europe, with 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 competitors in this regard. Some competitors introduced cloud-based SIEM

offerings two years ago, and have since adopted a cloud-first approach for new customers. Recent entrants into the SIEM market are cloud-native providers.

- **Branding:** LogRhythm takes a confusing approach to the naming of its product's components and capabilities. A more straightforward naming scheme would provide greater clarity to prospective buyers.
- **Move to the cloud:** LogRhythm faces the challenge of developing a new cloud-based platform and introducing its capabilities to buyers, while at the same time maintaining its legacy platform and executing its plans to migrate customers to the new platform.

ManageEngine

ManageEngine is a Niche Player in this Magic Quadrant. Based in Pleasanton, California, U.S., ManageEngine provides a number of security products, among which Log360 is its SIEM solution. Related solutions (or available modules) include Advanced Behavioral Analytics, Advanced Threat Analytics, Cloud Security Plus and DataSecurity Plus. Log360 is available as SaaS or on-premises, but does not support both in a hybrid model. Licensing is available on an annual subscription or a 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.
- **Limited deployment options:** ManageEngine Log360 supports either on-premises or cloud deployment in its Zoho cloud environment, not a hybrid mix.

McAfee

McAfee is a Niche Player in this Magic Quadrant. McAfee is headquartered in San Jose, California, U.S. Its customer base spans the world, but most of its clients are in North America. McAfee's Enterprise Security Manager (ESM) includes several components for logging and analytics. McAfee also has a large ecosystem of other security solutions that integrate with ESM, including Application Data Monitor, MVISION Cloud and MVISION EDR. There are perpetual licenses for physical or virtual appliances, and pricing is based on the appliance size (measured in cores) that can support a defined amount of data (measured in EPS). McAfee ESM Cloud, introduced in July 2020, is available on an annual subscription, priced by expected EPS.

Strengths

- **Hosted cloud offering:** McAfee ESM Cloud was released in 2020 to offer buyers another deployment option. It is a hosted version of ESM that uses Oracle Cloud, which has good coverage of most regions, including the Middle East.
- **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

Micro Focus is a Niche Player in this Magic Quadrant. It is headquartered in Newbury, U.K., and has offices and customers across the world. Its ArcSight SIEM platform consists of several components for event collection/logging, alerting, investigation, analytics and response. ArcSight customers are mostly large enterprises, with the remainder split evenly between small and midsize organizations. Customers are relatively evenly distributed across North America, Europe and Asia/Pacific, with smaller numbers in the Middle East and Africa and Latin America. Licensing

is primarily perpetual. Pricing is based on EPS. ArcSight Intelligence (UEBA) is available on a subscription basis, priced by number of users. Additional subscription options are planned.

Strengths

- **Modernization:** Micro Focus has reworked and modernized several components of its ArcSight architecture to support greater scalability and performance for data ingestion and management, improved reporting and a better UI. There is a roadmap for additional modernization.
- **UEBA and SOAR:** Micro Focus has improved ArcSight's integration with the Interset UEBA technology it acquired in 2019. In 2020, it acquired SOAR capability, which is already integrated into the platform.
- **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 programs.

Microsoft

Microsoft is a Visionary in this Magic Quadrant. Based in Redmond, Washington, U.S., Microsoft has a global base of customers. Its SIEM product, Azure Sentinel, became generally available in September 2019. It is delivered only as SaaS via Microsoft's Azure cloud services. Azure Sentinel is available in all Azure regions except China. Licensing is via subscription. Pricing is primarily based on the volume of data ingested, via reserved capacity or pay as you go. Use of services for extra data storage, automation and "build your own machine learning" incurs additional cost.

Microsoft has a large ecosystem of security solutions, such as endpoint protection platforms, EDR solutions and CASBs, that integrate with Azure Sentinel.

Strengths

- **Cloud-native SIEM product:** Since Azure Sentinel is cloud-native and built in Azure, it scales up and down elastically, as needed, to support users. Buyers do not have to worry about managing capacity, and license changes are not applicable, particularly with the pay-as-you-go option. Users can change their license model monthly. The pricing model aligns with a true SaaS approach, 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, as Azure Sentinel is an app that runs within Azure and relies on other Azure services to complement it (such as Log Analytics and Logic Apps). It is also important to understand how the different components of Azure Sentinel are priced and to manage their consumption, especially in a pay-as-you-go model.

- **Suitability of SaaS model for some buyers:** Some customers may be unable to take advantage of Azure Sentinel — for example, those seeking an on-premises solution because they have data residency requirements, or those that want a traditional licensing model (based, for example, on operational expenditure on a perpetual basis with maintenance included). It might actually be possible to fulfill data residency requirements with Azure Sentinel, but prospective customers need to examine the currently available Azure regions and investigate those that are planned.

NetWitness

NetWitness, an RSA business, is a Niche Player in this Magic Quadrant. NetWitness is headquartered in Bedford, Massachusetts, U.S. It has a global customer base of mostly large enterprises. The NetWitness Platform (NWP) includes NetWitness Logs, Network, Endpoint, IoT, UEBA and SOAR. Perpetual and term licenses are offered. Pricing of components is based on data volume (Logs and Network), number of endpoints (Endpoint), active accounts (UEBA), and users and playbooks (SOAR). 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 partner from the NetWitness ecosystem to provide a cloud option. NetWitness indicates that a hosted option is a near-term roadmap item.

- **Complexity:** NetWitness Logs and Network can be complex, depending on the architectural requirements, and may therefore prove challenging for organizations that are less mature and lacking resources. Buyers considering NWP should consider drawing on NetWitness' partner ecosystem for deployment and ongoing operational management support.

- **Cloud service monitoring:** NWP's support for CASB solutions is limited to Netskope and Proofpoint. Some popular SaaS apps, like those of Workday and Box, do not have native API integration support. CIPS like AWS, Azure and Google Cloud are supported, however. Other cloud services — from IBM and Oracle, among others — are supported, but not via API integrations. Nonintegrated SaaS and CIPS require the Universal Rest API Plugin, NetWitness' Log Collector or Log Decoder, a Python-based plug-in or a Logstash instance.

Odyssey

Odyssey is a Niche Player in this Magic Quadrant. Odyssey is based in Cyprus, and its operations are heavily focused on Europe and the Middle East. Odyssey provides a number of security solutions, 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.
- **Lack of some modern SIEM capabilities:** Odyssey is lacking in capabilities such as incident response, integration with service desk tools (although ServiceNow is supported), and support for common SaaS solutions and CIPS.
- **Extremely limited support for cloud services and application monitoring:** Odyssey supports only the Microsoft Graph API and Office 365 Management Activity API for monitoring Office 365, and deployment is limited to its own private cloud and Sahara Net.

Rapid7

Rapid7 is a Leader in this Magic Quadrant. Rapid7 is headquartered in Boston, Massachusetts, U.S. Its SIEM solution, InsightIDR, runs on the cloud-based Insight platform. Other products available include InsightVM (vulnerability management), InsightAppSec, InsightConnect (SOAR), DivvyCloud (cloud security posture management) and Enhanced Network Traffic Analysis. Customers of the InsightIDR platform are concentrated most heavily in the U.S., followed by Europe and Latin America. InsightIDR is offered on a term license, with a straightforward pricing model based on the number of assets monitored.

Strengths

- **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 specific to their environments and use cases should carefully assess whether Rapid7's out-of-the-box content and rule customization facilities meet their needs.

Securonix

Securonix is a Leader in this Magic Quadrant. Securonix is headquartered in Addison, Texas, U.S., and has offices elsewhere in the U.S., the U.K., Singapore and India. Its SIEM solution includes Next-Gen SIEM, Security Data Lake, UEBA, SOAR, NDR, threat intelligence, adversary behavior analytics and several use-case specific apps (such as for healthcare and SAP). Most Securonix customers are in North America, followed by Europe, Asia/Pacific, the Middle East and Africa, and Latin America. Customers are mostly large enterprises, but there are also some midsize customers. Smaller customers are served by managed service partners. Most buyers opt for term licenses, but perpetual licenses are available.

Strengths

- **Data privacy controls:** Securonix provides extensive controls to support data privacy, including granular role-based access control, extensive data masking flexibility and a workflow for unmasking.
- **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

Splunk is a Leader in this Magic Quadrant. Headquartered in San Francisco, California, U.S., Splunk has a global but U.S.-centric customer base. Splunk SIEM includes the core product, Splunk Enterprise, and Splunk Cloud, Enterprise Security and Mission Control. Premium, but not natively integrated, offerings exist for UEBA and SOAR. Splunk's offering can be deployed as software or via Splunk Cloud. Splunk Enterprise and Enterprise Security are licensed on subscription, with pricing models that include volume ingested per day, infrastructure/workload, tiered pricing and enterprise license agreements. In October 2020, Splunk released Mission Control as a SaaS-based solution for central visibility of Splunk Enterprise Security, User Behavior Analytics (UBA) and Phantom.

Strengths

- **Support for buyers wanting core SOC tools to support existing technology investments:** Splunk's approach will appeal to buyers who want a core platform that provides SIEM, UEBA and SOAR solutions, along with integration with a variety of third-party technologies. Splunk is flexible for buyers who require out-of-the-box integrations and support, which Splunk provides via its Splunkbase apps, APIs, Mission Control Plug-in Frameworks, and Phantom integrations.

- **New pricing models to address different usage patterns:** Splunk has expanded its license models over the past several years to offer buyers options beyond data-ingestion-based pricing. New options include workload-based pricing (using virtual CPUs on-premises and virtual compute units 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.

Sumo Logic

Sumo Logic is a Visionary in this Magic Quadrant. Headquartered in Redwood City, California, U.S., Sumo Logic also has offices in Europe (including the U.K.) and Asia/Pacific. Most of Sumo Logic's SIEM customers are in North America, with the next-largest concentrations being in Asia/Pacific and Europe. Its SIEM product is called Cloud SIEM Enterprise, which is available only as an AWS-based SaaS offering. Licensing is subscription-based (with pricing based on data ingestion) or credit-based (with credits being used to enable specific resource usage, such as for occasional search or continuous analytics), with tiering options.

Strengths

- **Pricing model flexibility:** Sumo Logic offers a pricing model with three elements: credit-based pricing, data tiering and solution packaging. This gives customers the flexibility to select the pricing scheme that best matches their planned data ingestion and investigation workloads, independent of the event rate and numbers of data sources or users.

- **Cross-customer visibility and insights:** Sumo Logic's multitenant architecture enables anonymized analytics across the customer base to improve the tuning of detections and workflows. Some of these capabilities may not be immediately visible to buyers, but can result in 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.

Venustech

Venustech is a Niche Player in this Magic Quadrant. Venustech is based in Beijing, China. Most of its customers are in Asia/Pacific, with smaller numbers in the Middle East and Africa. Its SIEM product is Venusense Unified Security Management. Related solutions (or available modules) include Cybersecurity Situation Awareness, Security Analytics, NTA, Configuration Verification, Business Supporting Security Management, and Asset Exploration and Management. The SIEM product is available as SaaS and on-premises. Licensing is perpetual or subscription-based, with special licensing for MSSPs and for organizations in the education sector. Pricing is based on the number of log sources, but pricing by number of employees is an option for SaaS models.

Strengths

- **Differentiated access to regions and countries:** Venustech offers this by working with Chinese state-owned enterprises, which many Western SIEM vendors have little or no access to.
- **Advanced batch and stream processing technologies:** Venustech uses these to enable advanced security analytics, such as UEBA features (offered as an add-on), and to provide functionality so that users can create their own analytics.
- **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, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Elastic
- Gurucul
- Huawei
- Microsoft
- Odyssey
- Sumo Logic
- Venustech

Note also that NetWitness, a stand-alone business within RSA, replaces Dell Technologies (RSA).

Dropped

- AT&T Cybersecurity, which now positions its SIEM offering as a service delivery platform.
- 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's product had to support data capture and analysis from heterogeneous, third-party sources (that is, sources other than the SIEM vendor's own products and SaaS), including market-leading network technologies, endpoints, servers, and cloud (IaaS or SaaS) and business applications.

- The vendor had to have SIEM revenue (product/SaaS license and maintenance revenue, excluding revenue from training, professional and managed services) exceeding $50 million for the 12 months prior to 30 September 2020, or have 250 end-user production customers, or have added 50 new logo end-user production customers as of the end of the same period. Production customers were defined as those who had licensed the SIEM offering and were monitoring production environments with it.

- The vendor had to receive 15% of its SIEM product/SaaS revenue for the period 1 October 2019 through 30 September 2020 from outside the region in which it had headquarters, and have at least 15 end-user production customers in each of at least two of the following regions: North America, Europe, the Middle East and Africa (EMEA), Asia/Pacific, Latin America.

- 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.
- **HanSight:** This vendor did not meet the commercial requirements for inclusion in this Magic Quadrant. It was acquired by Qihoo 360 Technology in June 2020.
- **Logsign:** This vendor did not meet the commercial requirements for inclusion in this Magic Quadrant.
- **Netsurion:** This vendor's EventTracker solution is positioned more as a service delivery platform than as an end-user SIEM solution.
- **SolarWinds:** This vendor did not meet the requirement for analytics capabilities.

Evaluation Criteria

Ability to Execute

Product or Service: This criterion evaluates a vendor's ability to provide product functions in areas such as real-time security monitoring, security analytics, incident management and response, reporting, and deployment simplicity, and its track record of doing so.

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 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

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 (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 show the highest degree of market understanding can adapt to customers' requirements in areas such as early targeted attack and breach detection, as well as simplified implementation and operation, while also meeting compliance reporting requirements.

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, service, 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. Development plans during the next 12 to 18 months are also evaluated. The SIEM market is mature — there is little differentiation between most vendors in areas such as support for common network devices, security devices, OSs and consolidated administration capabilities. We assign higher weightings to coverage of emerging event sources, such as IaaS and SaaS, and environmental context.

Despite vendors' focus on expanding their capabilities, we continue to value simplicity of deployment and ongoing support. Users, especially those with limited IT and security resources, still value this 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 for SIEM, and their growth is driven primarily by demand for threat management and secondarily by compliance requirements. Our overall evaluation of vendors in this Magic Quadrant includes an evaluation of their sales and support strategies for those regions, as well as product features to support local and regional compliance requirements for data residency and privacy.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓

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

Source: Gartner (June 2021)

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 evidence of superior vision and execution for emerging and anticipated requirements. They typically have a relatively high market share and/or 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 modestly sized SIEM customer base, and products that meet a subset of the market's general requirements. As the SIEM market

has matured, the number of Challengers has dwindled, to the point that there are none in this edition of the Magic Quadrant. Challengers typically have strong execution capabilities, as evidenced by financial resources and a significant sales and brand presence. However, Challengers either do not demonstrate a complete set of SIEM capabilities or lack a track record of competitive success with SIEM technologies comparable to the track records of Leaders.

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 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:

- Collection of security event information from a wide variety of sources in a central repository, where it can be processed and stored in various forms (such as, raw version, enriched and normalized).
- Real-time and historical analysis, and alerting to potential threats.
- Reporting and dashboards.
- Searching across historical data for forensics and threat hunting.
- Workflow and case management.
- Integrations and automation to extend the value proposition and enable more functionality.

SIEM technology is typically deployed to:

- Monitor, correlate and analyze activity across multiple systems and applications.
- Discover external and internal threats.
- 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 response) remains the primary driver, with general monitoring and compliance being secondary. In North America, many new deployments are undertaken by organizations with limited security resources but requirements to improve monitoring and breach detection, often at the insistence of larger customers or business partners. Most SIEM buyers regard support for compliance reporting as a bare minimum.

Larger companies that are conservative adopters of technology are also deploying SIEM. These large, late adopters — as well as many smaller organizations — value simplicity of deployment and operational support, and have therefore fueled interest in cloud-based SIEM delivered as a service. We continue to see organizations of all sizes reevaluate their SIEM vendors in order to replace SIEM technology associated with incomplete, marginal or failed deployments, or to offer better analytics and automation support for analysts undertaking investigation and response activities.

The SIEM market is mature and competitive. During this phase of broad adoption, multiple vendors can meet the basic requirements of typical customers. The greatest area of unmet need concerns effective detection of, and response to, targeted attacks and breaches. Effective use of threat intelligence, behavior profiling and analytics can improve detection success. SIEM vendors continue to increase their native support for behavior analysis capabilities, as well as their integrations with third-party technologies, and Gartner customers are increasingly expressing

interest in developing 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 capabilities that meet the functional requirements for SIEM, and now fulfill the market criteria for inclusion in this Magic Quadrant. There are several vendors with smaller market shares that generate strong interest among Gartner customers, due to their strength in supporting analytics-focused use cases or their SaaS consumption model, or both. Other vendors are of interest to distinct market segments, such as buyers of their other products, buyers with geographic preferences, and buyers seeking add-on monitoring services from a technology provider.

SIEM Services

Many Gartner clients indicate that they are seeking external service support for their SIEM deployment, or that they plan to acquire that support in conjunction with a SIEM product. Many indicate a lack of internal resources to manage a SIEM deployment, a lack of resources to perform real-time alert monitoring or a lack of expertise to expand a deployment for new use cases. We expect demand by SIEM users for such services to continue to grow as more customers face 24/7 monitoring requirements and implement use cases that require deeper SIEM operational and analytics expertise. We also expect increased interest in acquiring use-case content via third-party vendors, such as SOC Prime, or the user communities associated with several SIEM products.

SIEM vendors have moved to address customer resource shortages in several ways. By offering SIEM as SaaS, vendors have eliminated the need for customers to maintain the underlying 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 protection, detection and response products for endpoints, networks and the cloud (see Innovation Insight for Extended Detection and Response). They are configured by their vendors to provide automated threat detection and response capabilities within the scope of those products. XDR platforms may provide curated, largely “hands off” detection and response capabilities for organizations that can commit to a single-vendor approach and accept the vendor-defined and vendor-managed threat detection and response options. Organizations need to understand how they might cover use cases that cannot be addressed by XDR products. Interestingly, as XDR technology evolves, Gartner is seeing some vendors, such as FireEye, Gurucul, McAfee and Securonix, treat their SIEM solution as part of an XDR offering — a trend we expect to continue.

- **Managed detection and response services:** There is a broad range of delivery styles for these services, but the focus is the provider’s investigation, validation, and presentation of containment and remediation advice for security events, rather than the escalation of lightly triaged alerts to the customer. Increasingly, providers are able to offer, and customers are willing to accept, actions to contain or disrupt events, typically via endpoint or network-based controls. These providers vary in their abilities to monitor a customer’s range of security controls and to collect logs for compliance reporting. For further details, see Market Guide for Managed Detection and Response Services.

Evaluation Criteria Definitions

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, 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.