

GARTNER MAGIC QUADRANT FOR SIEM



In order to provide the latest updates surrounding the [security](#) information and event management- SIEM- market, leading research group [Gartner](#) releases a yearly report with the top vendors for organizations to consider: Gartner Magic Quadrant for Security Information and Event Management (SIEM).

Defined by the customer's need to analyze event data in real-time for the early detection of attacks, the SIEM market is also a vital component of collecting, storing, analyzing, investigating, and reporting on event data for incident management and regulatory compliance purposes. Based on their ability to execute platforms as well as their completeness of vision, Gartner has evaluated the strengths and weaknesses of the SIEM vendors it considers most significant in the current market.

In order to be considered for Gartner's SIEM Magic Quadrant, vendors must offer both SEM (real-time monitoring and incident management) and SIM (log management, analytics, and compliance reporting). These vendors must support data capture from a variety of data sources, such as security programs, network devices, and security devices, as well as deliver their product as a software, an appliance-based product, or an as-a-service model.

The Magic Quadrant for SIEM 2017 can be seen below, showcasing Leaders, Visionaries, Niche Players, and Challengers:

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (December 2017)

Leaders in the SIEM Magic Quadrant 2017

In choosing the Leaders for the SIEM Magic Quadrant, Gartner explained, "In addition to providing technology that is a good match to current customer requirements, Leaders also show evidence of superior vision and execution for emerging and anticipated requirements. They typically have relatively high market share and/or strong revenue growth, and have demonstrated positive customer feedback for effective SIEM capabilities and related service and support."

Leader in the SIEM market stand out for advanced threat detection, security monitoring, and incident response capabilities. These vendors included in the Leaders Magic Quadrant include IBM, Splunk, McAfee, and LogRhythm.

Key Takeaways from the Report

Multiple strengths were identified in choosing the top leaders in the Security Information and Event Management Magic Quadrant:

- Wide variety of deployment options, including on-premise, in the cloud, or the hybrid model
- Full suite of security-focused solutions offering easy integration across heterogeneous

ecosystems

- Provides replacement of outdated SIEM deployments while delivering the most innovative security analytics solutions on the market
- All products comprised of use-case-agnostic data analysis and prepackaged security-specific queries, visualizations, and dashboards

Conclusion

Each year, the appeal of SIEM continues to broaden as it shifts focus from strictly compliance towards threat management. With the need for [cybersecurity](#) at an all-time high, detection with SIEM can provide greater visibility into a variety of environments, giving your organization the preventative measures it requires. Choosing a SIEM provider can be challenging, but utilizing the Gartner SIEM Magic Quadrant is an excellent place to start.

Download the full [report](#) to:

- Learn where the market stands and where it's going
- Evaluate vendor strengths and compare scores on various criteria

How do I use a Gartner Magic Quadrant?

Gartner's Magic Quadrant is the first step to understand the technology providers you might consider for a specific service. Depending on the types of investments you are looking to make, each quadrant has its own benefits and advantages.

How does a Gartner Magic Quadrant work?

Utilizing a graphical illustration, a Gartner Magic Quadrant provides a snapshot of four types of technology providers that can help you best meet your business goals:

- Leaders- Competitive providers that are known to execute well against their current vision and are often innovative giants in their industry
- Visionaries- Full of providers that understand where the future market is going or have a strong vision for where it will end up
- Niche Players- Highly focused on a small segment
- Challengers- Often dominate a large segment

Magic Quadrants help you:

- Quickly understand the market's competing technology providers as well as their ability to innovate and provide options for the future
- Understand how providers are competitively positioned and the strategies they are using to compete for end-user business
- Compare a technology provider's strengths and challenges with your specific needs and business goals