IDC MarketScape

IDC MarketScape: Worldwide SIEM for Enterprise 2024 Vendor Assessment

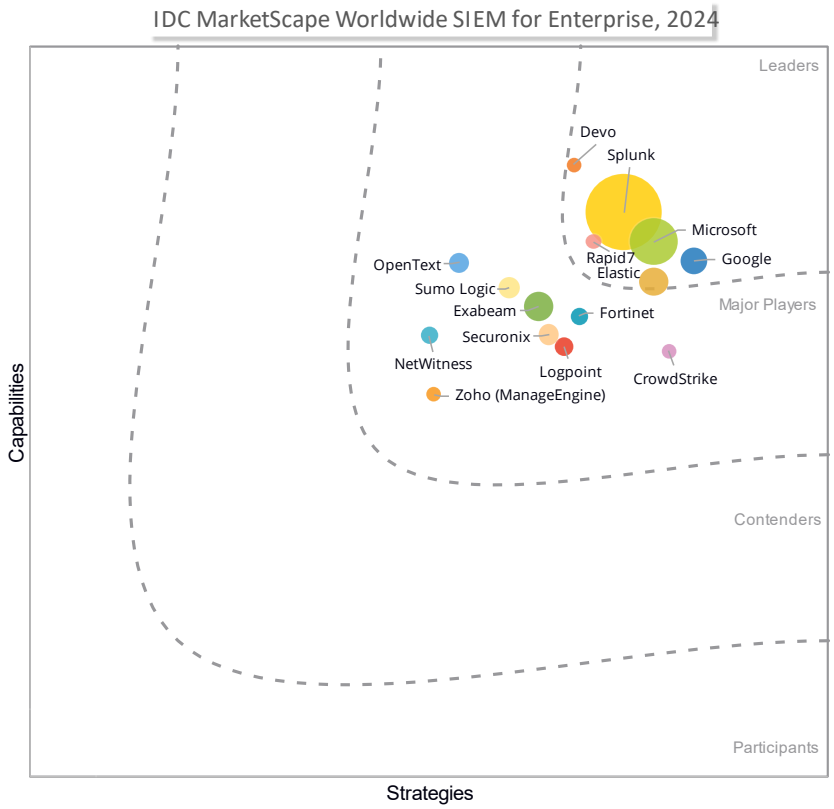
Michelle Abraham

THIS IDC MARKETSCAPE EXCERPT FEATURES ELASTIC

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide SIEM for Enterprise Vendor Assessment



Source: IDC, 2024

September 2024, IDC #US51541324e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide SIEM for Enterprise 2024 Vendor Assessment (Doc # US51541324). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1, 2 and 3.

IDC OPINION

Although security information and event management (SIEM) platforms have existed for more than 20 years, the SIEM of today has moved far beyond the log aggregation and storage upon which it was founded. Today's SIEM monitors the log data for anomalies and suspicious events triggering alerts based on unusual behavior and detection rules. It often serves as the workspace for security analysts to investigate incidents that are correlations of alerts with other contexts such as asset information, vulnerabilities, and threat intelligence. IDC expects that in the future, the SIEM will also be the response center of the SOC with automated handling of many incidents via playbooks. Generative AI (GenAI) assistants will be used to query the data, summarize information, and draft reports, connectors, detection rules, and playbooks to reduce some of the complexity in operating a SIEM. Last, they will guide analysts on next steps.

In mid-2024, several major changes occurred among the vendors that offer SIEM platforms. Mergers, acquisitions, and vendors leaving have changed the competitive landscape of the SIEM market. Despite its maturity as a piece of technology, the market remains dynamic. According to IDC's January 2024 *Worldwide Views on SIEM Survey,* the top feature for organizations with more than 2,500 employees is a real-time detection engine so alerts are generated as quickly as possible. The next most important feature is a cloud-native SIEM architecture followed closely by out-of-the-box (OOTB) connectors from vendors to connect to all the data sources the organization wants to ingest. While some organizations do want to stay with an on-premises SIEM, many are moving to one of the many cloud-native options. Since each customer environment is different with varied sets of security tooling, SIEM vendors need to offer a wide set of data connectors to best serve customers.

The top challenge for organizations with more than 2,500 employees is needing staff dedicated to the SIEM — one reason cloud SIEMs have proven popular since they remove the need for the customer to manage the SIEM infrastructure. Other high-ranking challenges are lack of workflow automation and time-consuming investigation

processes that require pivoting to multiple tools, which should encourage vendors to help customers with both guidance and action in investigation and response processes that are centralized in a single console.

Over the past several years, IDC has seen more vendors add the ability to construct and run playbooks directly from the SIEM. Alert correlation helps reduce the sheer volume of alerts, while auto-disposition of alerts due to correlation or other rules removes the need for analysts to check each and every alert. Generative AI assistants are offered to query the SIEM in natural language as well as offer guidance and summarization of activities and threat intelligence. The goal of vendors is to enable more efficient use of their SIEM.

SIEM vendors each have threat research teams that are producing content for the SIEM that customers can test and choose to apply in their SIEM as is or tune before use. The content includes detection rules, threat hunts, and playbooks. Additional content may come from a SIEM vendor's community where customers and users can exchange ideas or may be developed by third-party partners and placed in the SIEM vendor's marketplace.

The evaluation criteria emphasize capabilities that enable the security team to bring security telemetry from any system, apply detections to the data in a way that correlates information and prioritizes actions, and investigate to determine the appropriate response action.

IDC expects critical success factors for SIEM platforms for enterprise to be:

- OOTB connectors and vendor-supplied detection, threat hunt, and playbook content
- Automation built into the SIEM that does not rely on adding a SOAR
- Easy to understand and predictable pricing with few add-ons
- Guidance in the SIEM on how to investigate/respond to alerts
- Straightforward customer support plans that help customers receive more value from their SIEM over time
- Wide range of channel and MSSP partners
- Continued innovation and expansion in all the aforementioned areas

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Vendors had to meet the following criteria in order to be included in this assessment:

- The offering must be marketed as a SIEM, not XDR, network detection and response (NDR), log management, and so forth.

- The offering should be commercially available for use as a SIEM that is managed by the customer, not a vendor-managed SIEM.
- The SIEM must capture telemetry from multiple security sources/tools — it cannot be limited to one cloud or security platform.
- The product must have at least $50 million in revenue in CY23.
- The product must be offered and available on a worldwide basis with sales in a minimum of four global regions.

ADVICE FOR TECHNOLOGY BUYERS

The SIEM is often the centerpiece of an organization's security operations (SecOps) when used to its full extent, which makes it a complicated solution. These are some of the elements to consider:

- Think about your organization's needs for today and tomorrow. Data sources and ingestion only seem to grow, not shrink. Federated search and analytics as well as data orchestration to route and filter data may help manage SIEM costs by offering alternatives to ingesting all desired data into the SIEM.
- Consider the ease of deployment when you are thinking about starting with a new SIEM. Professional services can be a large part of SIEM costs.
- Evaluate your need for data retention and compliance reporting. Some vendors include at least a year of data retention in their basic offer.
- Analyze the potential for customer support help to realize more value from the SIEM through additional understanding of its potential as it is today and with features to come.
- Weigh the utility of user and entity behavioral analytics (UEBA) to track anomalous activity for detecting insider threat, account compromise, lateral attacks, data exfiltration, and other use cases.
- Assess the potential of a GenAI assistant to make life easier for inexperienced analysts.

VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Elastic

Elastic is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide SIEM for enterprise.

In the most recent fiscal year, Elastic's revenue was up 19% over the prior year with 16% revenue growth expected for the next fiscal year. Security is about 25% of annual contract value, while Elastic Cloud was 43% of the total for the year. Elastic Security, one of two out-of-the-box solutions from Elastic, was built on its own Elastic Stack using the Elasticsearch and Kibana components all around the open source Elastic Common Schema. All Elastic customers have access to the Elastic Security SIEM.

Elastic was one of the first vendors to offer a GenAI assistant; it first delivered the feature a year ago as part of its highest subscription tier. Unlike other SIEM vendors, Elastic has customers bring their own model, while its vector database is used for retrieval-augmented generation (RAG). Since Elastic is open, much of its documentation is readily available on the internet so customers can train their model or use retrieval-augmented generation for content. Over 300 customers are using its GenAI assistant in production today.

Today, Elastic Security is part of the Elastic Stack hosted option and is offered in more than 50 cloud regions and on the AWS, Azure, and Google Cloud Platform (GCP) marketplaces. Elastic Cloud Serverless, which is currently in preview and will be generally available in the fall 2024, is built on Search AI Lake, which is designed for low-latency applications including security. Search AI Lake is available today on AWS with expansion plans to other cloud service providers. Searchable snapshots can be stored in cheap storage outside of Elastic while still being searchable through the Elastic user interface (UI).

Attack discovery, launched in May 2024, uses AI to correlate alerts and present the full information in the UI to improve the security analyst workflow. It offers security teams a view of the most critical attacks. Elastic has recently changed its query language to a pipe query language called Elasticsearch Query Language (ES|QL), which is designed for all types of data. ES|QL improves the speed and efficiency of searches while enabling context enrichment with threat intelligence.

Internet threat research is conducted by the Elastic Security Labs team, which has also developed an LLM safety assessment and detection rules for GenAI threats. The Labs team is responsible for developing detection rules as well as proactively engaging customers when it sees novel threats in the customer environment.

Elastic uses a resource-based pricing model that depends on the amount of memory needed to run the cluster for all products including security, observability, and search

so customers can scale across their usage. Customers desiring faster storage may pay for more memory; the ratio of memory to storage makes up the ECU. Cloud customers that prefer ingest-based pricing do have that option. Elastic combines SIEM, EDR, and cloud security under a single Elastic Security SKU so add-ons like the Elastic Agent have no additional cost.

Strengths

- Customers can deploy Elastic Security on premises or in the cloud with the ability to search across all Elastic clusters from the same user interface no matter the site nor the region.
- Elastic has a popular community that submits detection rules, threat hunts, and playbooks; after review and testing, they may be integrated into existing Elastic content. Detection rules are open so customers can see the logic behind them.

Challenges

- Elastic does not currently integrate with any GRC platforms and does not support many of the compliance frameworks supported in other SIEM platforms. Customers can create their own custom integrations and query the data necessary to comply with various frameworks.
- Organizations are aware of Elastic for log storage but often not the full capabilities of its SIEM plus other security products. Elastic is expanding its marketing efforts in a move to improve visibility.

Consider Elastic When

Elastic's log management platform is the basis for the company's search, observability, and SIEM solutions. An organization can ingest data once either on premises or in the cloud and use it for multiple purposes across the three solutions.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

SIEM is a data platform used for policy and compliance assurance as well as to correlate alerts and initiate security investigations. SIEM solutions include products designed to aggregate data from multiple sources to identify patterns of events that might signify attacks, intrusions, misuse, or failure. Event correlation simplifies and speeds the monitoring of network events by consolidating alerts and logs into events or incidents. Products can also consolidate and store the log data that was processed by the SIEM. SIEM platforms can be queried to gather additional insights around security alerts/events as well as for threat hunting.

A SIEM platform must take in different logs and flows, have dashboards specifically used for threat investigation, and be capable of compliance reporting. In this sense, a SIEM is differentiated from security analytics products that are designed to allow users flexibility in specifying their particular security framework and running data against that framework in order to better analyze data. SIEM is different from threat intelligence products that are designed to take in a variety of threat intelligence sources and provide a platform for organizations to analyze their own data against a variety of different threat intelligence feeds. Often, companies will use business intelligence (BI) platforms in combination with open source platforms to index data, but IDC does not

count this as SIEM categorically. Ideally, a SIEM incorporates aspects of security and threat analysis, threat intelligence, business intelligence, and database management to provide search, storage, indexing and, most importantly, data that facilitates incident detection and response.

LEARN MORE

Related Research

- *IDC MarketScape: Worldwide SIEM for SMB 2024 Vendor Assessment* (IDC #US52038824, September 2024)
- *Costs of Switching SIEM Platforms* (IDC #US52411524, July 2024)
- *Why Do Customers Keep or Replace Their SIEM?* (IDC #US52342924, June 2024)
- *Metamorphosis in the Multitude of SIEMs* (IDC #lcUS52283024, May 2024)
- *SIEM Users Rank Important Features* (IDC #US52074224, May 2024)
- *SIEM User Challenges in the Age of AI* (IDC #US50635424, April 2024)
- *IDC Market Glance: Security Information and Event Management (SIEM), 1Q24* (IDC #US49126223, January 2024)

Synopsis

This IDC study provides a vendor assessment of those offering security information and event management (SIEM) platforms for enterprises. Using the IDC MarketScape model, we considered SIEM vendors based on quantitative and qualitative criteria that is important to enterprise organizations selecting an SIEM. The assessment is based on a comprehensive and rigorous framework that includes vendor and customer interviews to evaluate how each vendor stacks up, and the framework highlights the key factors that are expected to be the most significant for achieving success in the SIEM market over the short term and long term.

"SIEM vendors continue to add more features to answer customer challenges of staffing, lack of automation, and investigation processes that require pivoting to multiple sources of information," said Michelle Abraham, senior research director, Security and Trust at IDC. "Modern SIEM platforms correlate signals automatically, providing security analysts with the data needed for their investigations in a centralized interface and offering guidance on next steps and remediation."

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com