IDC MarketScape

IDC MarketScape: Worldwide SIEM 2022 Vendor Assessment

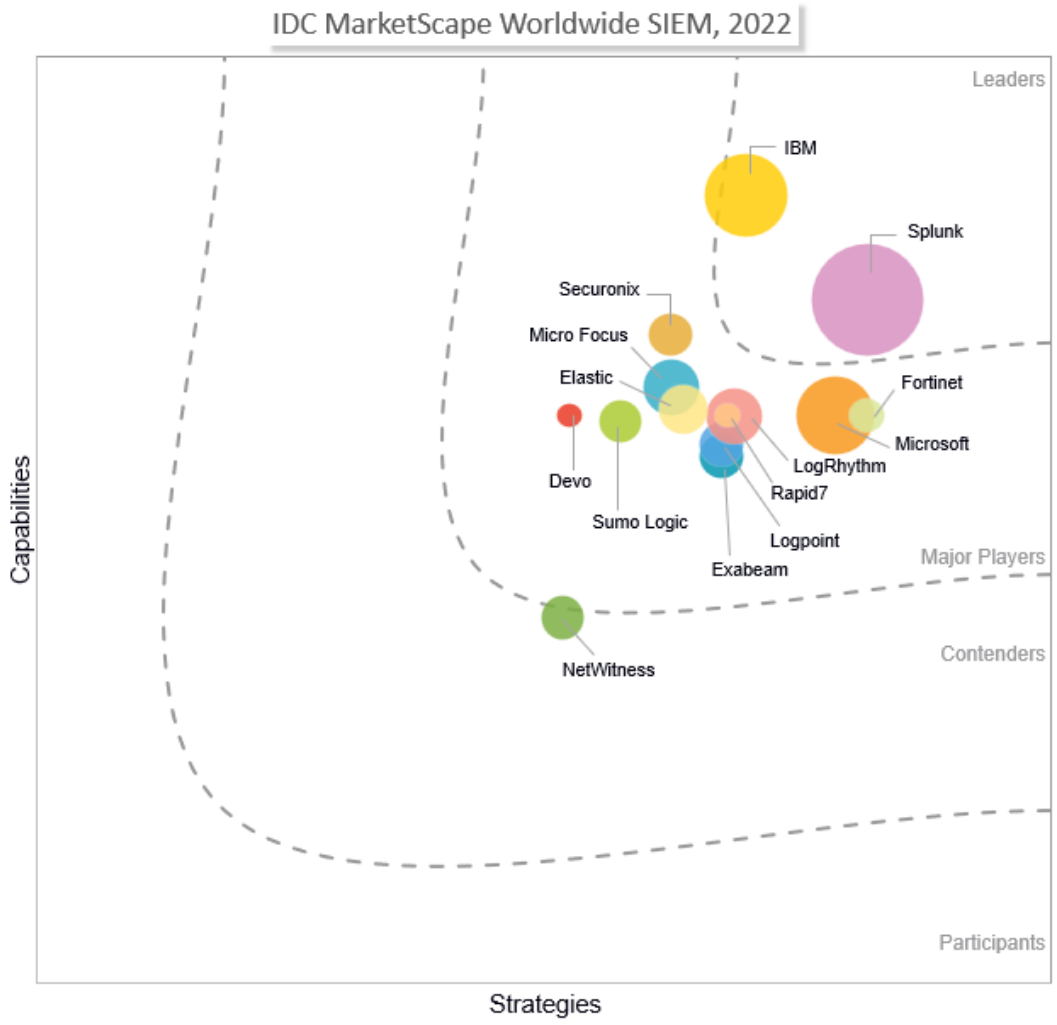
Michelle Abraham

THIS IDC MARKETSCAPE EXCERPT FEATURES DEVO

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape: Worldwide SIEM Vendor Assessment



Source: IDC, 2022

November 2022, IDC #US49029922ee

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 2022 Vendor Assessment (Doc # US49029922). 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.

IDC OPINION

Security information and event management (SIEM) is the central technology in many security operations centers (SOCs) as the collection point of telemetry data from the many other security tools in use such as firewalls, endpoint systems, cloud security systems, network detection systems, email security systems, and identity systems. The out-of-the-box (OOTB) data connectors that SIEM vendors offer are very important to customers in helping them bring their telemetry data into the SIEM so it can be correlated. However, each customer environment is different with varied sets of security tooling, so SIEM vendors need to offer a wide set of data connectors in order to best serve customers.

The cybersecurity talent shortage has organizations looking to automation to help them manage their security demands without exponentially expanding staff. Correlation of related alerts with threat intelligence helps reduce investigation time by presenting all known information in one place rather than requiring security analysts to pivot between systems and running searches for all the pieces of information needed.

Similarly, the shortage has organizations looking to their SIEM vendor for OOTB content such as the aforementioned data connectors as well as detection rules and playbooks that can be downloaded to their SIEM on a regular basis instead of requiring that the customer develop everything themselves. Many customers interviewed reported they used about 75% of the detection rules they downloaded as is while tweaking the rest for their particular environment.

SIEM is valued as a system to stop ransomware so the faster the information can be presented to security analysts the quicker their reaction time.

While all SIEM vendors have integrated with their own (if they have one) as well as third-party security orchestration automation and response (SOAR) vendors, a few have gone further in offering a full SOAR as part of the SIEM instead of as an add-on product.

The evaluation criteria emphasize capabilities and strategies that enable the security team to bring security telemetry from any system, apply detections to the data in a way that reduces false positives, and investigate to determine the appropriate response action without needing to dive into a large number of other tools. IDC expects critical success factors for SIEM platforms to be:

- OOTB data connectors that are updated for them when there is a change at the data source.
- New features on the road map that will alleviate analyst burnout from tedious investigation tasks, chasing false positives, and spending time on incidents that are less important.
- Pricing that allows customers to predict their costs without fear of overages and includes low-cost storage for logs that must be kept long term while remaining searchable.

- Easy deployment with quick-start guides to get up and running and readily available customer support options to deal with difficult issues.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

The inclusion criteria for this IDC MarketScape required vendors to have at least $50 million in annual revenue in 2021 — as determined by IDC — related specifically to SIEM platforms. Revenue had to come from more than one geographic region to be part of this worldwide evaluation.

ADVICE FOR TECHNOLOGY BUYERS

- The SIEM should have data connectors that enable data ingestion from the other tools in environment. If they do not exist, they will need to be written using your own internal or external resources, which are often limited either due to time constraints or budget. Consider the data to be ingested.
- Security data tends to grow rather than contract, with data being kept "just in case," so make sure the chosen SIEM vendor meets your scale and cost needs today and tomorrow.
- Low-cost storage options should be used for storage for "just in case" data that is not part of the everyday activity but may be useful for threat hunting or a forensic investigation. Make sure the SIEM search capability extends to this storage option without requiring the data be ingested into the SIEM again.
- The SIEM vendor community should be viewed as a first level of support because finding the answer in the community may be faster than waiting for the vendor response. The vendor marketplace is often a good source of content. Active as opposed to passive partnerships are revealed by the amount of content for each tool on the marketplace.
- Threat intelligence should be part of a SIEM offer with open source and paid options. The threat intelligence should be used to enrich the data in the SIEM and displayed within the user interface instead of requiring an analyst to flip to a different product to search for information.
- SIEM platforms have various degrees of response capabilities built in without needing an external SOAR. If you do not plan to use an external SOAR, investigate what your SIEM has in out-of-the-box playbooks. Along the same vein, some SIEM vendors include network analytics, endpoint agents, and machine learning (ML)-based user and entity behavior analytics (UEBA) as part of their package instead of requiring add-ons.
- Some SIEM vendors design their customer support for medium businesses while others are geared toward large enterprises. Understand how much hand-holding you will require and choose your SIEM vendor with this in mind.
- There are SIEM vendors that operate data analytics platforms with SIEM and other applications built on top like observability and application performance monitoring. It may make sense for your organization to work with a single vendor for all of these solutions.
- A MITRE ATT&CK framework visualization should show what tactics, techniques, and procedures (TTPs) are currently covered with log data being ingested into the SIEM. The framework normalizes the language of TTPs, so all vendors refer to issues the same way. A visualization will quickly show where there are gaps in detections so it can be determined if and what is necessary to close them.

VENDOR SUMMARY PROFILES

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.

Devo

Devo is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide SIEM software.

In June 2022, Devo announced Series F funding of $100 million with over $500 million raised overall. The latest round will be used to expand integration of the previously acquired Kognos and LogicHub platforms and to continue growth in new regions and verticals, including APAC and the public sector. Devo is currently considered FedRAMP "In Process" with full authorization expected in the fall of 2022.

Devo bought Kognos in April 2022, which is used today for autonomous threat hunting with the results gathered in an attack story. In the future, the Kognos technology will also be used to enrich the alert triage workflow and provide a risk score and, eventually, case creation and case resolution. Devo's plans for the autonomous SOC include removing many manual processes that cause analysts fatigue and boredom. In September 2022, Devo announced it was buying SOAR vendor LogicHub.

The Devo SciSec team brings together data science, threat research, and ML ability to produce content such as searches, alerts, ML models, and classifiers. The SciSec team is also creating attack simulations that customers can use to test their detections and defenses. Customers are also able to share in Devo's collective intelligence platform that allows anonymous insights into what threats other customers are seeing.

The Devo Exchange provides OOTB content including rules and Activeboards from Devo, partners, and the community that is curated by Devo. Content may be grouped into content packs. The Exchange is available within the platform; there is no need to exit it. Apps show what data sources are required to enable them and whether the source is currently present in the platform. Devo Connect is the online community launched in August 2022 where customers can learn from peers.

Devo has taken a no indexing data collection approach that makes adapting to changes in data formats easy as well as providing the ability to ingest any type of data. Customers have the raw data to use in machine learning models. Micro indexing happens asynchronously after ingestion. Data is tagged prior to ingest so the collection engine knows where to write the data. All data is compressed to help with Devo's costs. Queries run in real time and the platform is capable of running thousands of concurrent queries, which are the basis for all alerts, searches, dashboards, and reporting.

Strengths

- Devo offers 400 days of hot data storage as part of the platform, more than many other vendors.
- Devo offers a cloud-native SaaS, so customers do not have to manage their own infrastructure.
- In addition to Devo Security Operations, Devo also offers the Service Operations application; customers are able to use the same data for both security and IT observability purposes. The SaaS license is all inclusive of the platform, with add-ons for additional storage tiers.

Challenges

- Devo is less well known in the security industry, so it is working to improve brand awareness.
- As a younger SIEM vendor, Devo does not have as many OOTB collectors nor technology partners as other vendors.
- The Devo Platform pricing is based on ingest volume, which can be unpredictable.

Consider Devo When

Organizations that want a young, hungry company that receives positive feedback from customers for its flexibility and support should look at Devo. The vendor will be integrating newly acquired technologies to fulfill its vision of the autonomous SOC.

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

Security information and event management (SIEM) solutions are log-centric platforms used for policy and compliance assurance as well as to 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 error logs into a short, easy-to-understand package.

Products can also consolidate and store the log data that was processed by the SIEM. This technology also includes products that collect and disseminate threat intelligence, provide early warning threat services, and can provide information on countermeasures. The data from SIEM products is provided to policy and compliance solutions for consistent reporting.

A SIEM must take in different logs and flows, has dashboards specifically used for threat investigation, and is capable of compliance reporting. In this sense, 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 to better analyze data. And 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, SIEM incorporates aspects of security and threat analytics, threat intelligence, business intelligence, and database management to provide search, storage, indexing and, most importantly, data that facilitate incident detection and response.

LEARN MORE

Related Research

- *IDC PeerScape: SIEM Practices for Enabling a Trusted Tool* (IDC #US49688022, September 2022)
- *Worldwide Security Information and Event Management Market Forecast, 2022-2026: Dated Assumptions and New Innovations – Washing Away the SIEMs of the Past* (IDC #US48506322, September 2022)
- *Worldwide Security Information and Event Management Market Shares, 2021: The Cardinal SIEMs* (IDC #US48506522, July 2022)
- *IDC Market Glance: SIEM and Vulnerability Management, 2Q22* (IDC #US49009522, April 2022)
- *Features and Challenges in SIEM and Device Vulnerability Management Platforms: Variations by Size of Organization* (IDC #US48860222, February 2022)

Synopsis

This IDC study provides a vendor assessment of those offering security information and event management (SIEM) platforms. Using the IDC MarketScape model, we considered SIEM vendors based on quantitative and qualitative criteria that is important to 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 buyers need to consider the rest of their security environment when choosing an SIEM. Does the SIEM have integrations with tools in place or under purchase consideration? Does the pricing allow some level of predictability and options for data storage? Does the SIEM have built-in automations that allow analysts to reduce time spent on investigation, particularly on alerts that are false positives? Does the SIEM vendor offer the level of support that meets the buyer's maturity? All these are important considerations, which should drive buyers to check out SIEM vendors they may not have considered in their last purchase decision." – Michelle Abraham, research director, Security and Trust at IDC.

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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

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