Market Share

Worldwide Security Information and Event Management Market Shares, 2022: The Multitude of SIEMs

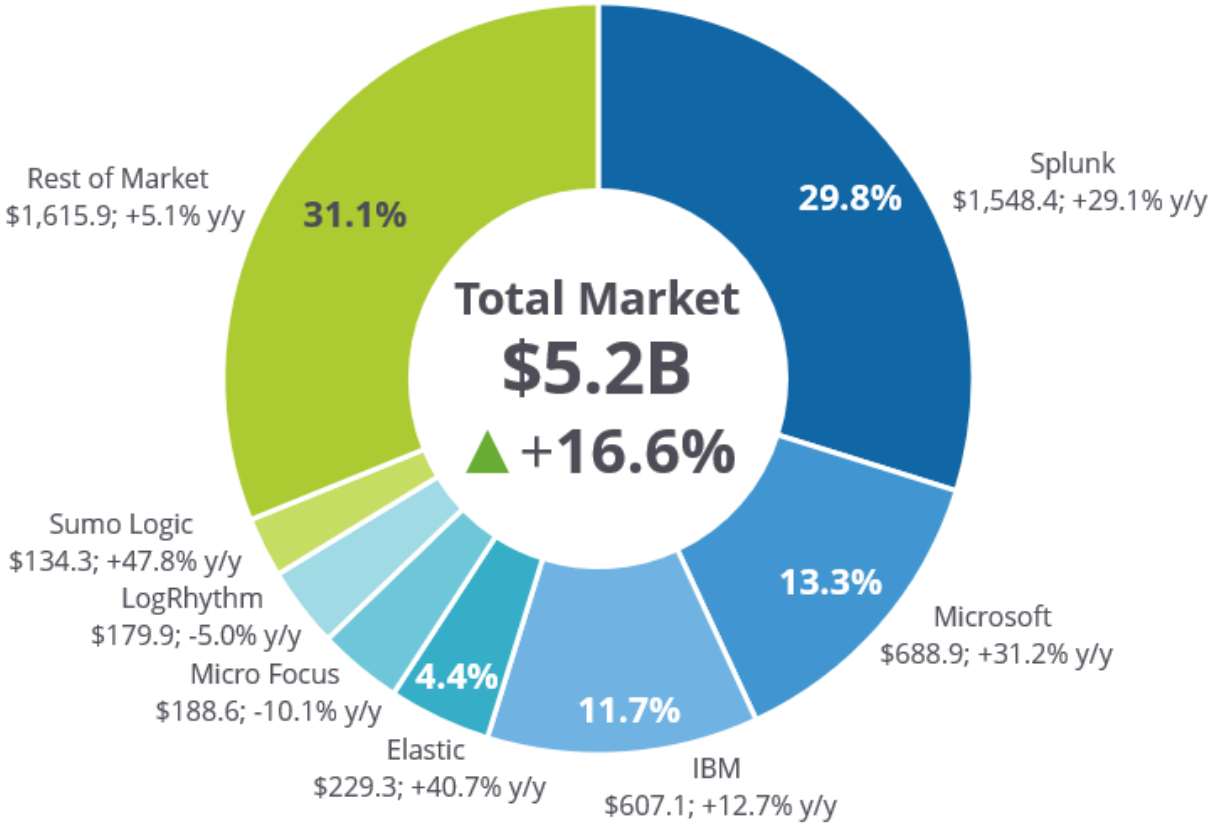
Michelle Abraham

THIS IDC MARKET SHARE EXCERPT FEATURES SPLUNK

IDC MARKET SHARE FIGURE

FIGURE 1

Worldwide Security Information and Event Management 2022 Share Snapshot



Note: 2022 Share (%), Revenue ($M), and Growth (%)

Source: IDC, 2023

July 2023, IDC #US51012523e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC Market Share: Worldwide Security Information and Event Management Market Shares, 2022: The Multitude of SIEMs (Doc # US51012523). All or parts of the following sections are included in this excerpt: Executive Summary, Market Share, Who Shaped the Year, Market Context, Appendix and Learn More. Also included are Figures 1, 2, 3, 4 and 5 and Table 1.

EXECUTIVE SUMMARY

The top vendor in the worldwide security information and event management (SIEM) market by revenue was Splunk in 2022, with a 29.8% share of the market. Its SIEM revenue grew by 29.1% compared with 16.6% for the overall market. Microsoft and IBM were second and third, respectively, exchanging places from 2021 while Elastic moved up two places to fourth.

SIEM vendors have been adding content and response capabilities to their SIEM to help their customers utilize the data they have been collecting. New common schema frameworks and data management using data lakes will make it easier for customers to switch SIEM vendors in the future, so improving customers' experience with their SIEM becomes even more important.

With the launch of ChatGPT in November 2022, the conversation around what generative artificial intelligence (AI) can do for cybersecurity has exploded. SIEMs have been paired with machine learning (ML) user and entity behavioral analytics (UEBA) for more than five years to detect anomalous behavior, but generative AI will help automate more tasks. Several SIEM vendors have announced generative AI products that will assist security analysts with investigation and reporting tasks.

This IDC study investigates the SIEM software market. It discusses overall market dynamics, analyzes the competitive landscape, and provides a quantitative assessment of the biggest vendors in the market.

"The reported demise of the SIEM market at the hands of XDR vendors is greatly exaggerated since the SIEM market saw double-digit growth of 16.6% in 2022 as vendors add to the functionality of their products," declared Michelle Abraham, research director, Security and Trust. "Generative AI arms SIEM vendors with transformative technology that will advance security analyst efficiency by offloading mundane tasks to machines and democratizing the institutional knowledge of the best tier 2 and tier 3 security analysts."

ADVICE FOR TECHNOLOGY SUPPLIERS

The main applications of the SIEM according to end users in the United States are shown in Figure 2.

FIGURE 2

Top Reported Use Cases for the Security Information and Event Management

n = 259

Source: IDC's *Security Operations Center Survey,* December 2022

Based on these use cases, vendors help their customers by doing the following:

- Develop threat hunts for your customers to easily add to their SIEM based on the latest attack vectors according to threat intelligence sources. Suggest threat hunts to users based on their recent searches.
- Include user behavior analytics in your SIEM and make it seamless to use across the environment. Suggest detection rules based on the user behavioral analytics data.
- Offer automated correlation of alerts to speed up incident investigations so security analysts need to do less searching themselves. Present the information in a visual timeline to make it easy to see the sequence of events.

MARKET SHARE

The worldwide revenue data for SIEM by vendors for 2020–2022 is shown in Table 1.

TABLE 1

Worldwide Security Information and Event Management Revenue by Vendor, 2020–2022 ($M)

	2020	2021	2022	2022 Share (%)	2021–2022 Growth (%)
Splunk	968.9	1,199.6	1,548.4	29.8	29.1
Microsoft	437.8	525.1	688.9	13.3	31.2
IBM	524.7	538.9	607.1	11.7	12.7
Elastic	90.3	163.0	229.3	4.4	40.7
Micro Focus	229.2	209.8	188.6	3.6	-10.1
LogRhythm	164.9	189.3	179.9	3.5	-5.0
Sumo Logic	72.1	90.9	134.3	2.6	47.8
Exabeam	65.5	87.3	124.0	2.4	42.0
LogPoint	69.9	82.4	112.5	2.2	36.4
Securonix	49.6	94.5	112.4	2.2	18.9
Other	1280.1	1273.1	1267.1	24.4	0.5
Total	3953.0	4453.9	5192.5	100.0	16.6

Source: IDC's Worldwide Semiannual Software Tracker, April 2023

Splunk continues its lead in the SIEM market in 2022, growing its revenue by 29.1%. Microsoft surpassed IBM for the second spot with 13.3% share while IBM moved to third with 11.7%. Elastic, Sumo Logic, Exabeam, and Datadog each grew revenue by more than 40% on a worldwide basis. Russian vendor Positive Technologies' more than 160% growth is due to other vendors pulling out of the Russian market.

IBM QRadar Suite was announced in April 2023, bringing IBM's endpoint detection and response (EDR)/XDR, SIEM, and SOAR products together under a single user experience offered as SaaS on AWS. The modules that are part of the QRadar Suite will have the same user experience across them, with prioritization based on risk and continuous updates from the X-Force Threat Intelligence team. The QRadar Suite will also be available as a software license for those not choosing SaaS. Strategic areas of focus for IBM are providing an open platform that allows customers to keep their security data

where they choose but make it accessible. Another area of focus is AI and automation to improve security analyst's productivity and expertise that can be shared across the team. The new QRadar Log Insights product offers log management with a scalable security data lake for more efficient analytics. The IBM Security QRadar Suite supports Amazon Security Lake.

OpenText completed its acquisition of Micro Focus and will continue using the ArcSight brand for its SIEM offering. In October 2022, LogRhythm announced its cloud-native Axon platform that was built from the ground up rather than on its existing software. With Axon, LogRhythm was able to ease log collection and improve search and visualization across the data. LogRhythm also continues to enhance the LogRhythm SIEM platform.

In May 2023, Francisco Partners, which also owns BeyondTrust, Checkmarx, Forcepoint, and iboss, closed on its $1.7 billion acquisition of Sumo Logic. At RSA, Sumo Logic introduced new UEBA functionality, Cloud SIEM Automation Service to bring automation to alert enrichment, and Cloud SIEM Insight Trainer, which uses ML to tune detection logic. With its observability product, Sumo Logic suggests its SIEM is suitable for application security teams as well as security operations.

Exabeam's Outcomes Navigator visualization tool is generally available in the New-Scale SIEM, which was announced in October 2022, to provide better visibility over its environment with an understanding of where coverage is in place and recommendations for improvement. Exabeam maintains its Common Information Model (CIM), which offers a common log format. Its New-Scale SIEM was built on a new cloud-native data back end that enables log processing at 1 million events per second. All Exabeam SIEM customers are able to take advantage of its continuous publication of correlation rules.

Headquartered in Europe, Logpoint is expanding its presence in South America in 2023. In March 2023, Logpoint released its AgentX endpoint agent to enable better malware detection and the ability to respond on the endpoint. AgentX joins UEBA, SOAR, and SIEM as part of Logpoint's converged SIEM platform. Summa Equity bought a majority stake in Logpoint, while Yttrium is a minority shareholder.

In April 2023, Securonix announced its Unified Defense SIEM, which includes the Snowflake Data Cloud to handle the data customers want to access with the SIEM, with 365 days of hot data storage all in a single tier. The Unified Defense SIEM also has threat detection content via a content library that is curated by the Securonix Threat Labs team as well as analytics capabilities to help customers map their detection coverage against MITRE ATT&CK and compliance frameworks. To help defensive efforts, the new SIEM also includes Securonix's Autonomous Threat Sweeper, curated intelligence from customers and partners, as well as bringing contextual data from internal and external sources within the investigation.

RSA has now split into several pieces with NetWitness as the threat detection and response entity, which offers the SIEM as well as XDR, NDR, SOAR, and EDR. A recent integration with AWS AppFabric will enable NetWitness customers to easily bring in SaaS application data into their security workflows. FortiSIEM is one of many products that are part of the Fortinet Security Fabric, which offers customers a platform that is tightly integrated with its other secure networking products. FortiSIEM has a built-in configuration management database to help customers monitor their assets and changes made over time. Link graph technology helps customers visualize the connections between devices, incidents, and users. One area of focus for Fortinet is OT security and this includes FortiSIEM.

Rapid7 is now marketing its InsightIDR platform as XDR and SIEM with a tiered pricing approach; InsightIDR Ultimate includes an InsightConnect license for unlimited SOAR ability, while InsightIDR

Advanced includes some automation workflows. One of Rapid7's differentiators is the company's managed services team is a large user of the platform providing Rapid7 with a continuous feedback loop over what is working and what is not.

Devo has made several acquisitions over the last year, including LogicHub for its SOAR in September 2022. In January 2023, Devo announced AI-based Devo DeepTrace developed with technology from its Kognos acquisition of 2022. DeepTrace helps with investigations by searching for additional detail around an alert to present the security analyst with the context. For threat hunters, DeepTrace helps with proactive threat hunting by enabling customization of provided hunt queries developed by Devo's SciSec team. At RSA, Devo announced it will support OCSF and therefore enable customers to use Amazon Security Lake.

WHO SHAPED THE YEAR

This excerpt was prepared for **Splunk** but also included the following vendors: Microsoft, IBM, Elastic, Micro Focus, LogRhythm and others.

The vendors that shaped the year include those at the forefront of several trends including AI, common schema, and use of data lakes.

Splunk

After revenue growth of 37% in fiscal 2023, Splunk started off fiscal 2024 with 16% year-over-year global annual recurring revenue (ARR) growth and 810 customers having total ARR of over $1 million. Revenue expectations are about $3.9 billion for fiscal 2024. The security business is accelerating particularly in the public sector and in the Asia/Pacific region. Enterprise Security Cloud is growing at an even greater pace.

Splunk continues to see customers migrate from ingest-based pricing to workload-based pricing, with workloads based on the ingest and search functionality usage. Writing efficient queries helps customers use the search resources more efficiently. Potential customers are able to get a sense of the Splunk cost with a public Splunk Virtual Compute (SVC) sizing calculator on the Splunk website. Inside the product, the Cloud Monitoring Console provides customers' information about Workload usage. The Splunk App for Chargeback provides visibility into how different groups within an organization are using the Splunk Cloud Platform.

To help customers use Splunk more effectively, Splunk is devising frameworks for specific use cases that customers may have. There are now frameworks for fraud and OT security. The Splunk for Fraud Analytics (SFA) app focuses on two strategic fraud use cases: account takeover and new accounts fraud. Using the risk-based alerting framework in Enterprise Security, SFA provides fraud prevention teams the ability to improve alert fidelity and reduce false positives and include default content such as fraud rules and dashboards. The Splunk for OT Security framework includes integrations with OT security vendors, audit and compliance coverage for North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), and an expansion of MITRE ATT&CK Matrix for Industrial Control Systems (ICS) tactics, techniques, and procedures. The frameworks accompany the analytic story and detection rule content that Splunk is offering in additional content for security customers. The detection rule creation is based on emerging threats or zero days that need a response. Support for SIGMA allows rules to be written in SIGMA and then translated to multiple formats.

Splunk is a member of OCSF and an AWS partner for Amazon Security Lake. With the general availability of Amazon Security Lake, Splunk now offers an add-on that allows customers to pull security events into Splunk from Amazon Security Lake that are already mapped to the OCSF schema.

To unify security operations, Splunk released the Splunk Mission Control app, which pulls in capabilities of the SIEM, SOAR, and threat intelligence platform that have previously been in separate silos. Splunk Mission Control provides a SOAR environment, which allows customers 100 response actions per day at no cost. Greater usage requires a separate SOAR license. In Splunk Enterprise Security 7.1, Splunk added streaming analytics with risk-based alerting for some insider threat use cases to augment its search-based alerting. It now offers threat topology visualization for a graph of relationships between assets, identities, and threat objects without the need to write queries.

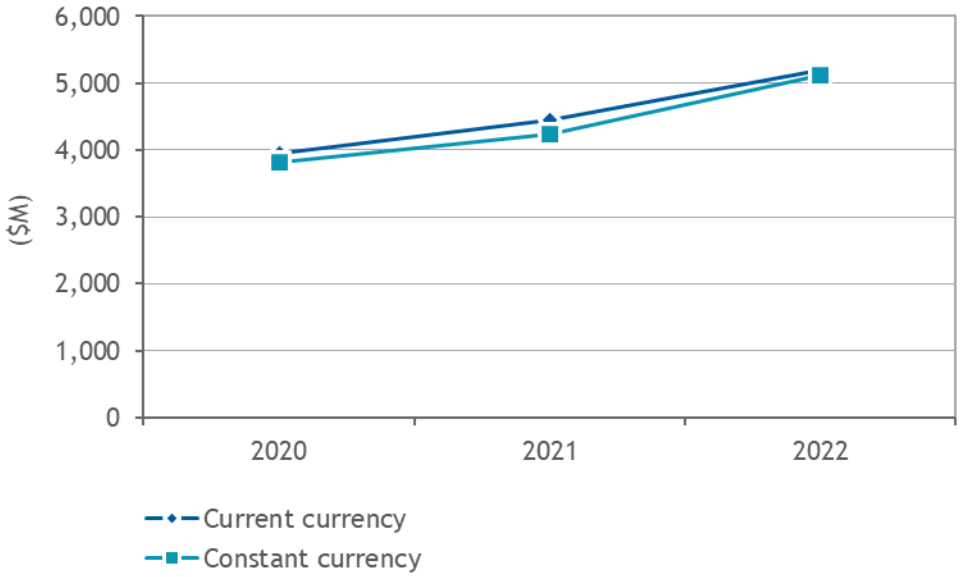
In November 2022, Splunk acquired TwinWave, and its product became Splunk Attack Analyzer. Splunk Attack Analyzer helps security analysts look at malware and credential phishing attacks with more efficient analysis of the threat, so action can be taken more quickly.

MARKET CONTEXT

Figures 3-5 provide additional information around the SIEM revenue in 2022.

FIGURE 3

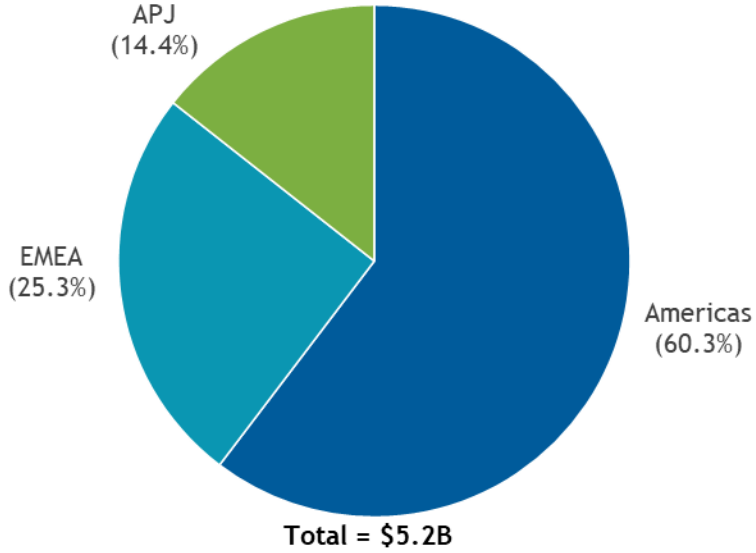
Worldwide Security Information and Event Management Revenue, 2020-2022: Current Currency and Constant Currency



Source: IDC's Worldwide Semiannual Software Tracker, April 2023

FIGURE 4

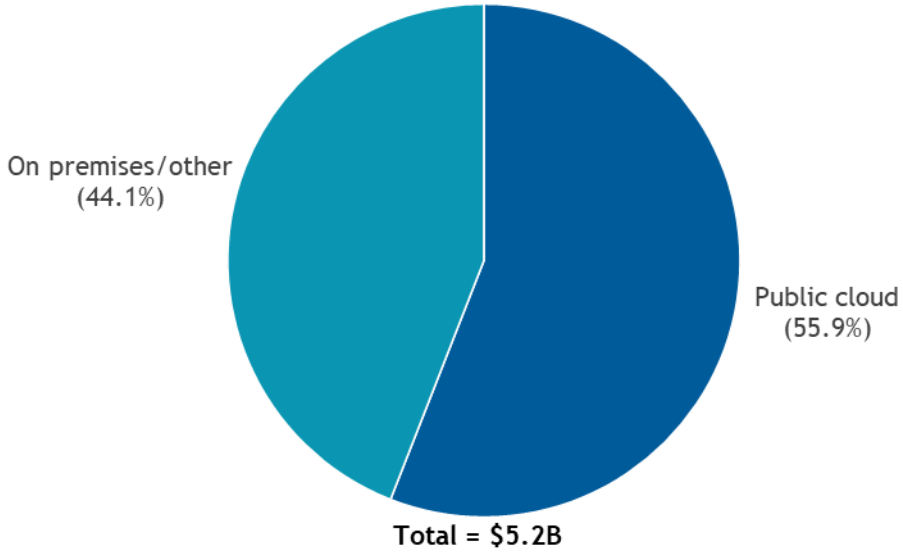
Worldwide Security Information and Event Management Revenue Share by Region, 2022



Source: IDC's Worldwide Semiannual Software Tracker, April 2023

FIGURE 5

Worldwide Security Information and Event Management Revenue Share by Deployment Type, 2022



Source: IDC's Worldwide Semiannual Software Tracker, April 2023

Significant Market Developments

OCSF

One of the complexities of the SIEM is the ingestion of data because each data source usually has different fields, which may be similar but named differently. The data coming from each source has to be mapped to the fields in the SIEM to make it helpful to the SIEM for searching, alerting, and correlating to other pieces of data.

The work is often done by the SIEM vendor or the vendor of the system that is the source of data, so out-of-the-box connectors are available to the customers of both systems. If a connector is not available, customers often have to do the work themselves; sometimes, they find it too complicated, so the log source is not ingested. If a connector breaks because the fields change, the work needs to begin again.

A SIEM vendor works with hundreds of partners, so making this process more efficient would benefit them. If all systems use the same schema, there is no need to normalize or translate data for each connector. The work would only need to be done once. However, it is not enough to be able to ingest the schema, but vendor platforms have to send data out in the schema. There are several efforts underway toward a common security schema, with the largest being the Open Cybersecurity Schema Framework (OCSF).

In 2022, several vendors combined efforts to produce a common schema framework that will make the data mapping process the same across vendors. The goal of the vendors is to simplify the exchange of data between the tools that ingest it, manage it, and enrich it, bringing more structure to security data, leading to greater efficiency and faster threat detection and response.

The 18 founding members of OCSF are AWS, Broadcom, Cloudflare, CrowdStrike, DTEX, IBM Security, IronNet, JupiterOne, Okta, Palo Alto Networks, Rapid7, Salesforce, Securonix, Splunk, Sumo Logic, Tanium, Trend Micro, and Zscaler. There are now more than 130 companies involved in OCSF, ranging from security technology vendors to financial firms to government agencies. The OCSF consortium has released Release Candidate 3 (RC3) for review. After the review, RC3 will become the generally available version 1.0 later in 2023.

Data Moves to the Data Lake

Now Amazon Security Lake is taking advantage of OCSF to create a single place for security data that does not have to be tied to a tool. It detaches security analytics from log storage; previously, the two went hand in hand. EDR, XDR, and SIEM vendors all include some amount of storage or retention time in their pricing today. The division of analytics and storage is likely to change the pricing dynamics of these systems since customers will pay vendors for their analytics and AWS for storage. It could even impact revenue at the analytic solution vendors. Vendors that offer workload pricing, like Splunk, have already planned for the separation. SIEM vendors that offer only price on ingestion will need to devise new pricing models.

The separation also removes a barrier to switching tools and even to switching vendors, because there will not be a cost to move the data if the customer moves to another vendor partnered with Amazon Security Lake. The data will still be in Amazon Security Lake. It also makes it easier to compare and contrast analytics tools such as SIEM and XDR to see which solution's queries best suit customer needs.

The shift to separate log management from security analytics seen in Securonix + Snowflake and Amazon Security Lake and its partners is going to mean substantial changes for SIEM and XDR vendors. The underlying data platform becomes much less important with analytics capabilities taking center stage. Outside of SIEM, the launch of Amazon Security Lake should encourage more security vendors to transform their log data into OCSF.

Strong New Competitor

Palo Alto Networks launched Cortex XSIAM, which brings together endpoint detection and response, network threat analytics (NTA), UEBA, cloud detection and response, attack surface management (ASM), SOAR, threat intel management, and case management to use the same data from sensors, logs, and threat intel feeds, in the fourth quarter of 2022.

Palo Alto Networks developed XSIAM from the learning in its own SOC and has commercialized this technology in the XSIAM product. Its SOC has been able to narrow down billions of events per day into hundreds of incidents, of which less than 10% require manual intervention, taking its mean time to remediation (MTTR) for high-priority alerts down to 1 minute.

XSIAM is designed to replace the SIEM with a unified back-end infrastructure that can handle the data Palo Alto Networks considers necessary for AI/ML responses as well as customers' own data sources. Once data is collected, XSIAM normalizes and correlates it to understand the relationships shown in the data while reducing the number of alerts, so the SOC is machine led with human oversight.

Workflows will be natively automated by XSIAM, instead of human-designed automation, to follow the steps of an SOC analyst. Automations are at the log level, not at the alert level, to provide more context. The AI will look at the different systems and data to figure out what is happening more quickly than humans, so response is faster, and breaches are disrupted mid attack.

During 2022, Palo Alto Networks had 10 customers as part of its XSIAM design partner (beta testing) program. For its second fiscal quarter of 2023, Palo Alto Networks announced $30 million in cumulative bookings since the launch. The vendor saw 100% bookings growth quarter over quarter in its most recent third fiscal quarter. The XSIAM sales focus is on Cortex XDR and Palo Alto Networks' firewall customers first and then to those with SIEM replacement projects, particularly organizations that want to move from on-premises to SaaS solutions.

METHODOLOGY

The cybersecurity market share document represents the summation of all 2022 reports as well as market trends known into June 2023. Importantly, the revenue estimates were derived in the same cycle as the Worldwide Security Tracker.

In this study, IDC is tracking several primary markets. This means that the revenue generated for one SKU can only be realized once (the revenue cannot be double counted in SIEM and policy and compliance, for instance). The second note is that there is revenue from physical appliances that is not represented in the Software Tracker but is captured in these market revenue estimates, although the revenue is a very nominal part of the whole industry.

The IDC software market sizing and forecasts are presented in terms of commercial software revenue. IDC uses the term *commercial software* to distinguish commercially available software from custom software. Commercial software is programs or code sets of any type commercially available through sale, lease, rental, or as a service. Commercial software revenue typically includes fees for initial and continued right-to-use commercial software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately. Upgrades may be included in the continuing right of use or may be priced separately. Commercial software must be available for competitive bidding. These use cases are counted by IDC as commercial software revenue.

Commercial software revenue excludes service revenue derived from training, consulting, and systems integration that is separate (or unbundled) from the right-to-use license but does include the implicit value of software included in a service that offers software functionality by a different pricing scheme. It is the total commercial software revenue that is further allocated to markets, geographic areas, and sometimes operating environments. For further details, see *IDC's Worldwide Security Products Taxonomy, 2023* (IDC #US49998922, January 2023).

As part of the cadence with this document and intimated previously, IDC sent revenue estimates to companies in this study for review and a chance to comment. Under no circumstance will IDC disclose the degree of transparency a vendor provided for a specific revenue estimate. Many companies may offer a precise revenue estimate or guide an analyst to 10-K/10-Q or related statements. Other companies are privately held or do not comment; others still provide ballpark estimates. In addition, the security team works with the larger tracker group, and we reconcile revenue to add to a larger whole. Other tools at the disposal of the analyst are contracts won, press releases, and number of employees. Otherwise, it is unfair and unethical to compromise the confidentiality of the participating vendors.

The data presented in this study is IDC estimates only.

Note: All numbers in this document may not be exact due to rounding.

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.

The formal definition of SIEM here is important for a couple of reasons and mostly for the reason of providing transparency. This term feels imprecise, but one of the criteria for a platform to be considered a SIEM is that it must drive like a SIEM. 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 though, 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.

RELATED RESEARCH

- *SIEM and Mature Versus Less Mature Security Operations: Differences Between Novices, Apprentices, Veterans, and Pacesetters* (IDC #US50436623, March 2023)
- *IDC Market Glance: SIEM and Vulnerability Management, 1Q23* (IDC #US50506123, March 2023)
- *IDC MarketScape: Worldwide SIEM 2022 Vendor Assessment* (IDC #US49029922, November 2022)
- *Worldwide Security Information and Event Management 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)

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