IDC MARKET SHARE

Worldwide Security Information and Event Management Market Shares, 2023

The Leaders in SIEM City

AUGUST 2024

IDC #US52525024E

Michelle Abraham

Sr. Research Director

Security and Trust

THIS MARKET SHARE EXCERPT FEATURES SPLUNK

About this Excerpt

The content for this excerpt was taken directly from IDC Market Share: Worldwide Security Information and Event Management Market Shares, 2023, The Leaders in SIEM City (Doc # US52525024, August 2024).

Worldwide Security Information and Event Management Market Shares, 2023

Abstract

This IDC presentation examines the market shares of the largest vendors in the worldwide SIEM market. It discusses overall market dynamics, looking at the significant developments in the SIEM market of the past year.

"The worldwide SIEM market continued its growth trajectory in 2023 with an increase of 14.6%, while GenAI assistance led the list of new features that are now available."

Lead Study Author:

Michelle Abraham

Sr. Research Director

Security and Trust

Market Definition

A 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 SIEM. SIEM platforms can be queried to gather additional insights around security alerts/events as well as for threat hunting.

Table of Contents

Worldwide Security Information and Event Management Market Shares, 2023

1 Executive Summary

2 Advice for Technology Suppliers

3 Market Share

4 Who Shaped The Year

5 Market Context

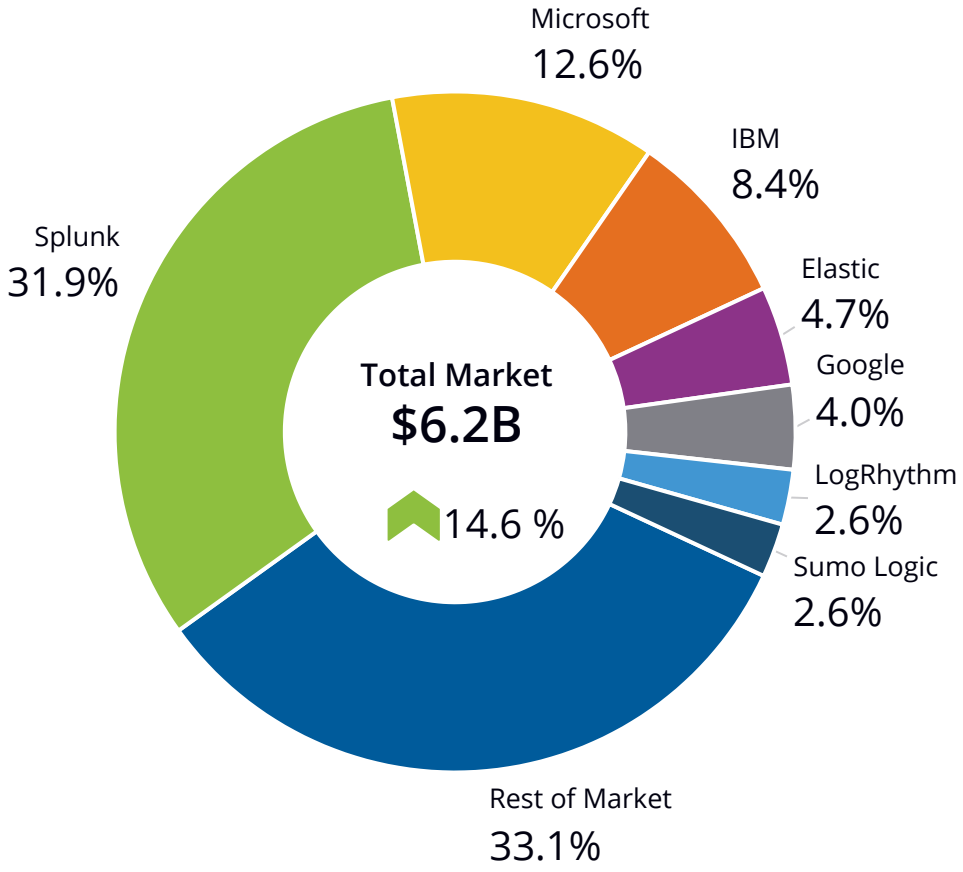
6 Methodology

Definitions

7 Related Research

Executive Summary

Worldwide Security Information and Event Management 2023 Share Snapshot

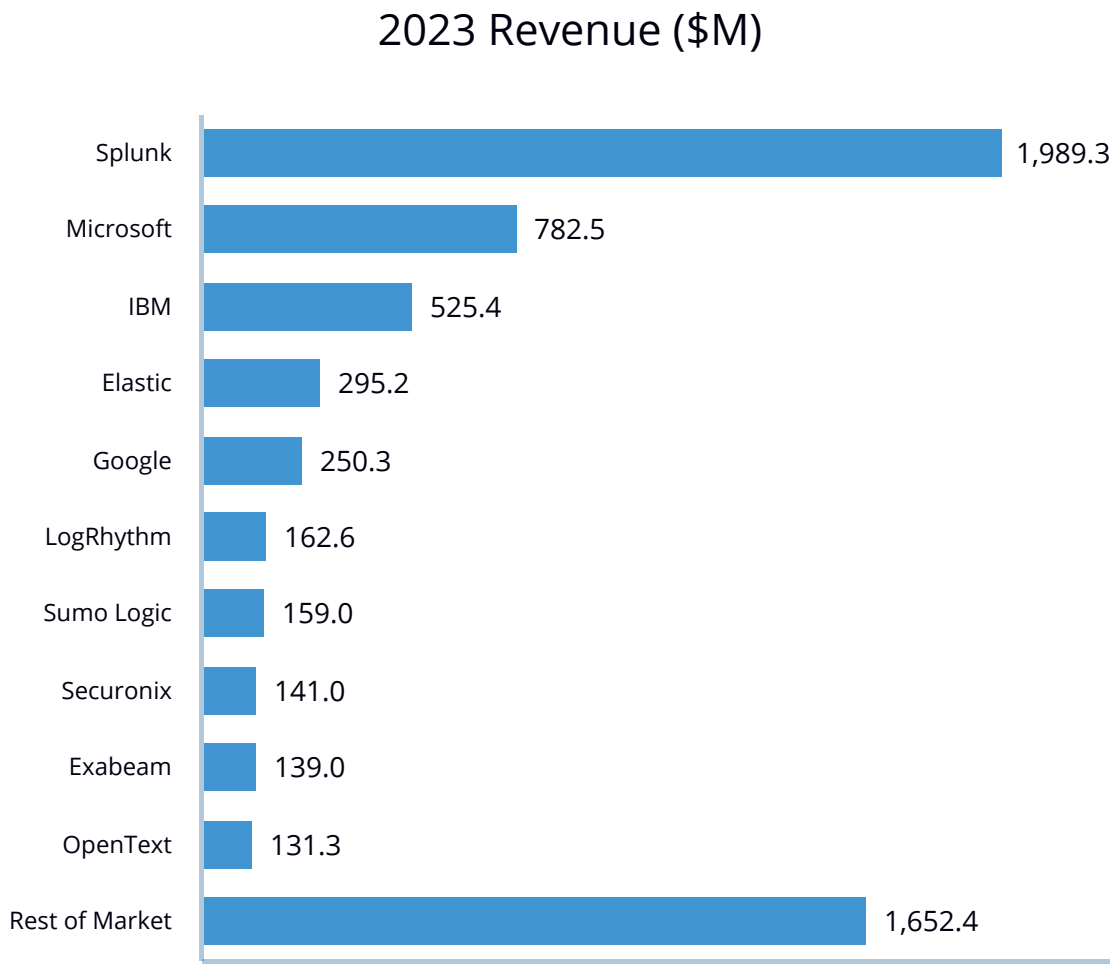


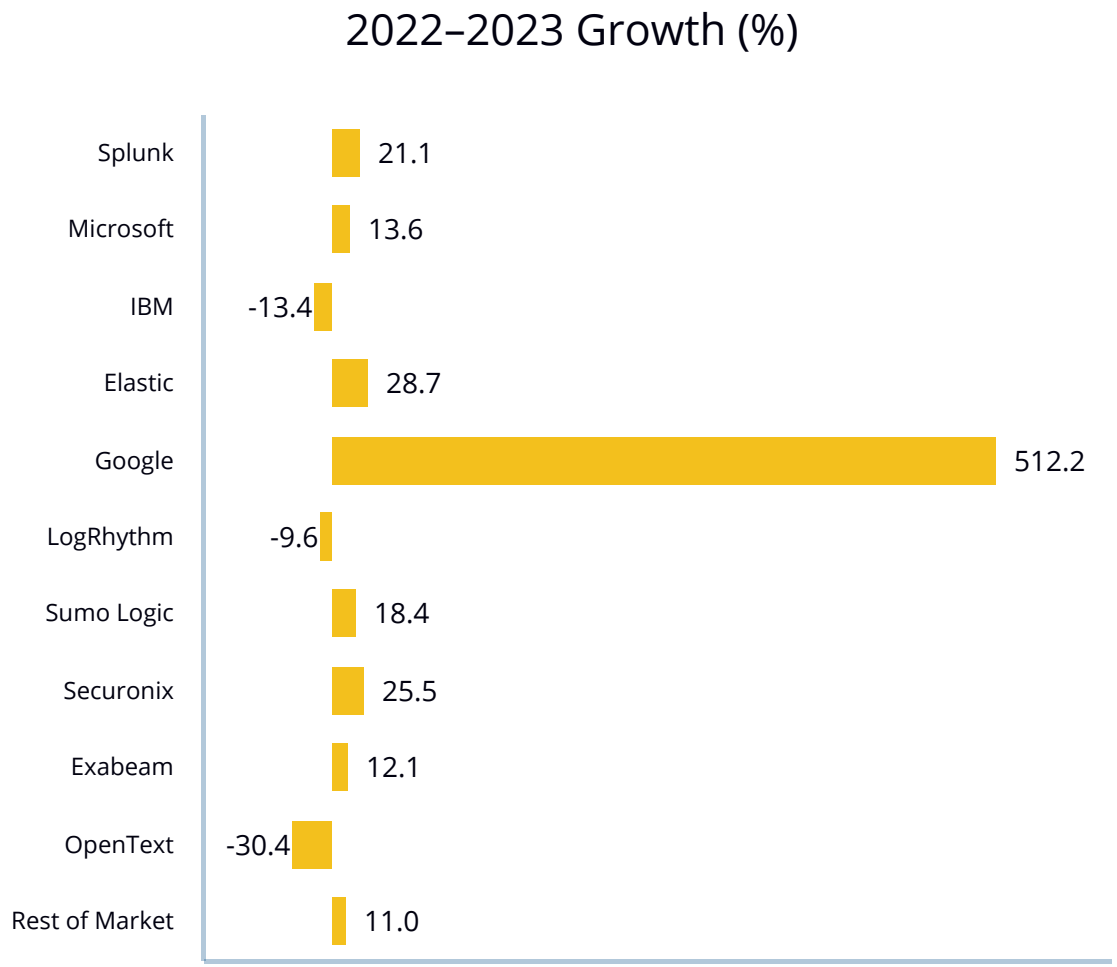
- **Splunk is on top for the fourth year in a row.**

Source: IDC, August 2024

Executive Summary

Worldwide Security Information and Event Management 2023 Share Snapshot





Source: IDC, August 2024

Advice to Technology Suppliers

Vendors of SIEM platforms should consider the following recommendations:

Facilitate the operation

Needing staff dedicated to SIEM is the greatest challenge for end users. Provide best practices and ongoing training.

Offer automation

Automatically correlate alerts with other alerts and threat intelligence to save investigation time.

Provide content

Detections, playbooks, and threat hunts help users get started even if they end up tuning for their environment.

Help customers mature

There are many use cases for SIEM, often too many to implement at the start. A maturity model plus understanding customer needs will improve the value customers receive from SIEM.

Take advantage of GenAI

Enable customers to query in natural language, and summarize actions with AI-written reports.

Market Share

Worldwide Security Information and Event Management Revenue by Vendor, 2021–2023 ($M)

Vendor	2021	2022	2023	2023 Share	2022–2023 Growth
Splunk	1,209.2	1,643.0	**1,989.3**	**31.9%**	+21.1%
Microsoft	525.1	688.9	**782.5**	**12.6%**	+13.6%
IBM	538.9	606.4	**525.4**	**8.4%**	-13.4%
Elastic	163.0	229.3	**295.2**	**4.7%**	+28.7%
Google	6.9	40.9	**250.3**	**4.0%**	+512.0%
LogRhythm	189.3	179.9	**162.6**	**2.6%**	-9.6%
Sumo Logic	90.9	134.3	**159.0**	**2.6%**	+18.4%
Securonix	94.5	112.4	**141.0**	**2.3%**	+25.4%
Exabeam	87.3	124.0	**139.0**	**2.2%**	+12.1%
OpenText	213.0	188.6	**131.3**	**2.1%**	-30.4%
Rest of Market	1,362.4	1,489.0	**1,652.5**	**30.4%**	**11.0%**
Grand total	**4,480.8**	**5,436.6**	**6,228.1**	**100.0%**	+14.6%

Splunk. Cisco sees the acquisition of Splunk as an opportunity for revenue expansion partly via the growth in sales capacity as well as integration with Cisco products such as Cisco XDR and Cisco Talos threat intelligence.

Source: IDC, August 2024

Market Context

Significant Market Developments

1. **GenAI assistants are widely available.** Many of the SIEM vendors have introduced GenAI assistants for their products. The most common use cases are querying systems in natural language and summarizing threat intelligence, investigation guidance, response tasks, and incident reporting.

2. **Proactive detection combines with reactive offerings.** Google and Palo Alto Networks are integrating proactive tooling such as attack surface management into their SIEM offers. Splunk introduced Asset and Risk Intelligence for asset discovery as a SIEM-adjacent solution. Rapid7's Threat Complete bundle combines its InsightIDR SIEM with the InsightConnect SOAR and InsightVM vulnerability management solution.

3. **SIEM vendors have their own threat research teams.** These vendor teams develop detection rules, threat hunts, and playbooks based on their internal and external threat intelligence feeds.

Market Context

Significant Market Developments

4 **UEBA and SOAR are frequently integrated into SIEM offers.** Previously sold as add-ons, many SIEM vendors have created bundles that include this functionality.

5 **Threat hunting is automated.** More vendors have developed solutions to handle this task for customers who may not have the time or the expertise to do so themselves.

6 **Correlation and case management are common features.** Most vendors offer case management and rules-based correlation in their SIEM instead of requiring customers to use a SOAR.

Methodology

The data presented in this document are IDC estimates only.

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 codesets 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. These 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.

Most IDC documents on software will include data on the migration of software products and revenue from traditional on-premises/other software to public cloud services. Note that the public cloud services revenue estimates in the software tracker agree with IDC's revenue estimates for proprietary and open source intellectual property–based software-as-a-service (SaaS) and platform-as-a-service (PaaS) offerings contained in the Public Cloud Services Tracker. They exclude third-party intellectual property-based SaaS and PaaS offerings.

Bottom-up/company-level data collection for calendar year 2023 began in January 2024 with in-depth vendor surveys and analysis to develop detailed 2023 company models by market, geographic region, and, in some cases, operating environment.

The worldwide software market includes all commercial software revenue across all functional markets or market aggregations. For further details, see *IDC's Worldwide Software Taxonomy, 2024* (IDC #US52000924, April 2024).

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

Methodology
Definitions

- ### User and Entity Behavioral Analytics

  User and entity behavioral analytics (UEBA) uses machine learning to detect anomalous behavior on the part of human and machine users as well as other entities that are part of an organization's environment. The capability is useful in detecting unknown threats because it is not operating with predefined threat determinants. One use case for UEBA is detecting insider threat.

- ### Security Orchestration Automation and Response

  Security orchestration is a method of connecting security tools and integrating disparate security systems. Orchestration is the connected layer that streamlines security processes and powers security automation, which enables an organization to maximize the productivity of its scarcest security resource — people — by reducing frequent and repetitive tasks generated within a given workload. Automated functions dynamically institute playbooks, trigger the download of proper patches, and then initiate a vulnerability assessment scan.

Related Research

Worldwide Security Information and Event Management Market Shares, 2023

Document title	IDC Document Number	Publication Date
Costs of Switching SIEM Platforms	US52411524	July 2024
SIEM Users Rank Important Features	US52074224	May 2024
IDC's Macroeconomic Forecast Assumptions, April 2024	US52097924	May 2024
IDC's Worldwide Software Taxonomy, 2024	US52000924	April 2024
SIEM User Challenges in the Age of AI	US50635424	April 2024
IDC Market Glance: Security Information and Event Management (SIEM), 1Q24	US49126223	January 2024
Worldwide Security Information and Event Management Forecast, 2023–2027: In the Face of XDR, Many Organizations Are Still Living in SIEM	US50271823	August 2023
Worldwide Security Information and Event Management Market Shares, 2022: The Multitude of SIEMs	US51012523	July 2023