

Grid[®] Report for Security Orchestration, Automation, and Response (SOAR) | Winter 2025



SOAR Software

Contenders									Leaders
Niche									High Performers

Satisfaction

Market Presence

G2 Grid[®] Scoring

(Security Orchestration, Automation, and Response (SOAR) Software continues on next page)

Security Orchestration, Automation, and Response (SOAR) Software (continued)

Security Orchestration, Automation, and Response (SOAR) Software Definition

Security orchestration, automation, and response (SOAR) software products are tools used to help integrate security technologies and automate incident-related tasks. These tools integrate with a company's existing security solutions to help users build and automate workflows, simplifying the incident response process and reducing the amount of human intervention necessary to handle security incidents. Companies use these tools to create a centralized system complete with visibility into a company's security software and operational processes. These tools also reduce the time it takes to respond to incidents, as well as the potential for human error in remediating security threats and vulnerabilities.

SOAR platforms combine aspects of [vulnerability management](#), [incident response](#), and [security information and event management \(SIEM\)](#) solutions. SOAR products are designed to provide some of each tool's respective functionality or integrate with third-party tools. Once integrated, processes can be designed to identify incidents and automate remediation tasks.

To qualify for inclusion in the Security Orchestration, Automation, and Response (SOAR) category, a product must:

- ▶ Integrate security information and incident response tools
- ▶ Allow security professionals to build response workflows
- ▶ Automate incident management and response tasks within workflows
- ▶ Provide formalized incident, workflow, and performance reports

Security Orchestration, Automation, and Response (SOAR) Grid® Scoring Description

Products shown on the Grid® for Security Orchestration, Automation, and Response (SOAR) have received a minimum of 10 reviews/ratings in data gathered by November 19, 2024. Products are ranked by customer satisfaction (based on user reviews) and market presence (based on market share, seller size, and social impact) and placed into four categories on the Grid®:

- ▶ Products in the Leader quadrant are rated highly by G2 users and have substantial Market Presence scores. Leaders include: [KnowBe4 PhishER/PhishER Plus](#), [Microsoft Sentinel](#), [Tines](#), [Torq](#), [ServiceNow Security Operations](#), and [Swimlane](#)
- ▶ High Performing products have high customer Satisfaction scores and low Market Presence compared to the rest of the category. High Performers include: [Barracuda Incident Response](#), [Logpoint](#), [Blink](#), [Blumira Automated Detection & Response](#), [CrowdSec](#), [SIRP](#), and [Shuffle](#)
- ▶ Contender products have relatively low customer Satisfaction scores and high Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. Contenders include: [Palo Alto Networks Cortex XSOAR](#), [Google Security Operations](#), [Splunk SOAR \(Security Orchestration, Automation and Response\)](#), and [IBM Security QRadar SOAR](#)
- ▶ Niche products have relatively low Satisfaction scores and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. Niche products include: [Demisto](#), [n8n](#), [Intezer](#), [Sumo Logic](#), [D3 Security](#), and [LogicHub](#)

Grid® Scores for Security Orchestration, Automation, and Response (SOAR) Software

The table below shows the Satisfaction and Market Presence scores that determine product placement on the Grid®. To learn more about each of the products, please see the profile section.

Leaders

	# of Reviews	Satisfaction	Market Presence	G2 Score
KnowBe4 PhishER/PhishER Plus	328	93	85	89
Microsoft Sentinel	138	61	99	80
Tines	201	79	62	70
Torq	97	82	57	69
ServiceNow Security Operations	10	63	53	58
Swimlane	40	51	54	53

High Performers

Barracuda Incident Response	11	63	47	55
Logpoint	28	52	40	46
Blink	11	58	25	41
Blumira Automated Detection & Response	24	62	14	38
CrowdSec	30	56	14	35
SIRP	19	62	5	34
Shuffle	15	59	6	32

(Grid® Scores for Security Orchestration, Automation, and Response (SOAR) Software continues on next page)

* Products are ordered by G2 Score. Satisfaction score is used as a tiebreaker if two products have the same G2 Score.

Grid® Scores for Security Orchestration, Automation, and Response (SOAR) Software (continued)

The table below shows the Satisfaction and Market Presence scores that determine product placement on the Grid®. To learn more about each of the products, please see the profile section.

Contenders

	# of Reviews	Satisfaction	Market Presence	G2 Score
Palo Alto Networks Cortex XSOAR	18	47	64	56
Google Security Operations	26	37	71	54
Splunk SOAR (Security Orchestration, Automation and Response)	29	44	61	53
IBM Security QRadar SOAR	21	24	65	45

Niche

Demisto	15	42	44	43
n8n	16	45	31	38
Intezer	38	48	27	37
Sumo Logic	37	43	30	36
D3 Security	42	34	28	31
LogicHub	11	0	19	9

* Products are ordered by G2 Score. Satisfaction score is used as a tiebreaker if two products have the same G2 Score.

Grid® Methodology

Grid® Rating Methodology

The Grid® represents the democratic voice of real software users, rather than the subjective opinion of one analyst. G2 rates products from the Security Orchestration, Automation, and Response (SOAR) category algorithmically based on data sourced from product reviews shared by G2 users and data sourced from third parties.

Technology buyers can use the Grid® to help them quickly select the best products for their businesses and to find peers with similar experiences. For sellers, media, investors, and analysts, the Grid® provides benchmarks for product comparison and market trend analysis.

Grid® Scoring Methodology

The Grid® Report for Security Orchestration, Automation, and Response (SOAR) | Winter 2025 is based on reviews collected through November 19, 2024. We apply unique algorithms to this data to calculate Satisfaction (v4.0) and Market Presence (v7.0) scores for the Winter 2025 report quarter. To view the Security Orchestration, Automation, and Response (SOAR) Grid® with the most recent data, please visit the [Security Orchestration, Automation, and Response \(SOAR\)](#) page. For more details on Grid® Scoring, please view the [G2 Scoring Methodology here](#).

Grid® Categorization Methodology

Making G2 research relevant and easy for people to use as they evaluate and select business software products is one of our most important goals. In support of that goal, organizing products and software companies in a well-defined structure that makes capturing, evaluating, and displaying reviews and other research in an orderly manner is a critical part of the research process.

To manage the process of categorizing the software products and the related reviews in the G2 community, G2 follows a publicly available [categorization methodology](#). All products appearing on the Grid® have passed through G2's categorization methodology and meet G2's category standards.

Many terms that appear regularly across G2 and are used to aid in product categorization warrant a definition to facilitate buyer understanding. These terms may be included within reviews from the G2 community or in executive summaries for products included on the Grid®. A [list of standard definitions](#) is available to G2 users to eliminate confusion and ease the buying process.

Rating Changes and Dynamics

The ratings in this report are based on a snapshot of the user reviews and third-party data collected by G2 up through November 19, 2024. The ratings may change as the products are further developed, the sellers grow, and as additional opinions are shared by users. G2 updates the ratings on its website in real time as additional data is received, and this report will be updated as significant data is received. By improving their products and support and/or by having more satisfied customer voices heard, Contenders may become Leaders and Niche sellers may become High Performers.

Trust

Keeping our ratings unbiased is our top priority. G2 follows defined community guidelines to ensure privacy, and authenticity for users and reviews. For more details, please view the [G2 Community Guidelines here](#).

(Grid® Methodology continues on next page)

** Net Promoter, Net Promoter System, Net Promoter Score, NPS and the NPS-related emoticons are registered trademarks of Bain & Company, Inc., Fred Reichheld and Satmetrix Systems, Inc.



Grid® Methodology (continued)

Grid® Inclusion Criteria

All products in a G2 category that have at least 10 reviews from real users of the product are included on the Grid®. Inviting other users, such as colleagues and peers, to join G2 and share authentic product reviews will accelerate this process.

If a product is not yet listed on G2 and it fits the market definition above, then users are encouraged to [suggest its addition](#) to our [Security Orchestration, Automation, and Response \(SOAR\) category](#).

Product Profiles

Product profiles and detailed charts are included for products with 10 or more reviews.



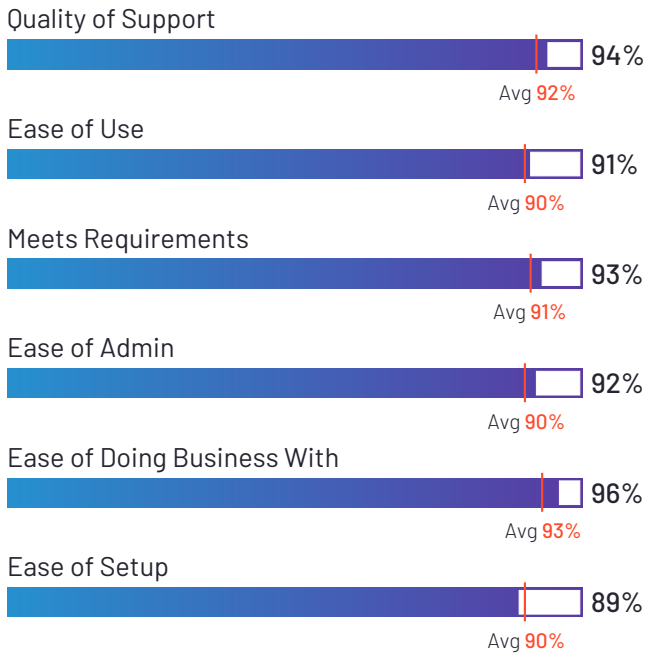
KnowBe4 PhishER/PhishER Plus

4.6 ★★★★★ (471)

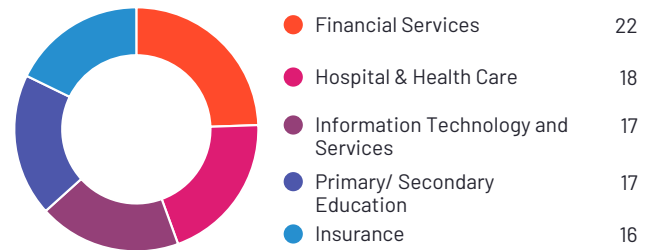


KnowBe4 PhishER/PhishER Plus has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. KnowBe4 PhishER/PhishER Plus received the highest Satisfaction score among products in Security Orchestration, Automation, and Response (SOAR). 98% of users rated it 4 or 5 stars, 94% of users believe it is headed in the right direction, and users said they would be likely to recommend KnowBe4 PhishER/PhishER Plus at a rate of 92%. KnowBe4 PhishER/PhishER Plus is also in the Incident Response category.

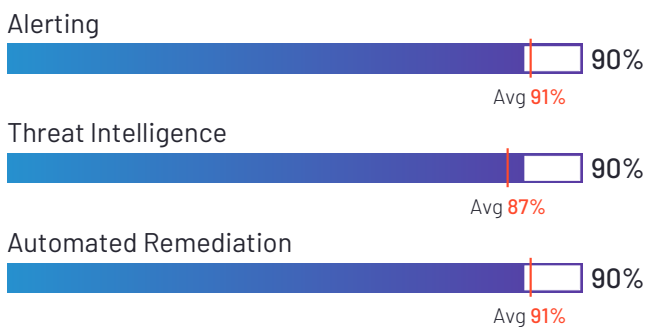
Satisfaction Ratings



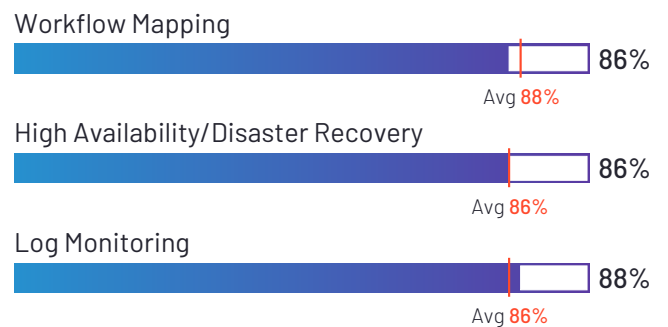
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
KnowBe4, Inc.



HQ Location
Clearwater, FL



Year Founded
2010



Employees (Listed On LinkedIn)
1,934



Company Website
knowbe4.com



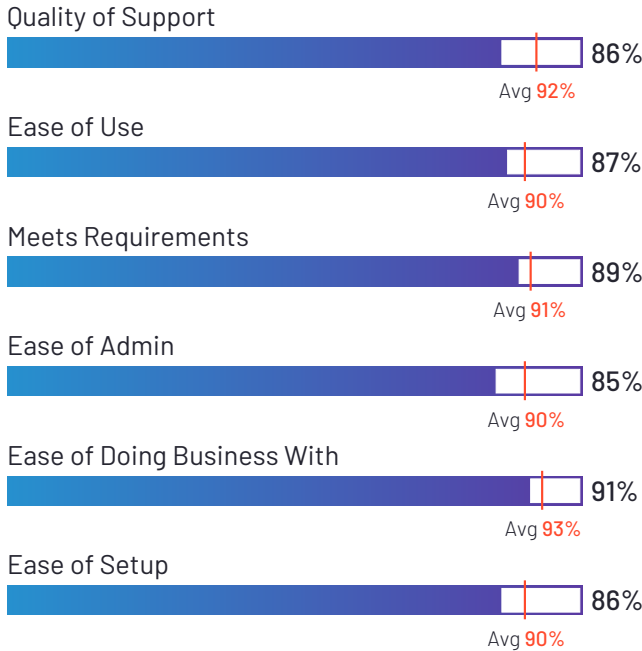
Microsoft Sentinel

4.4 ★★★★★ (288)

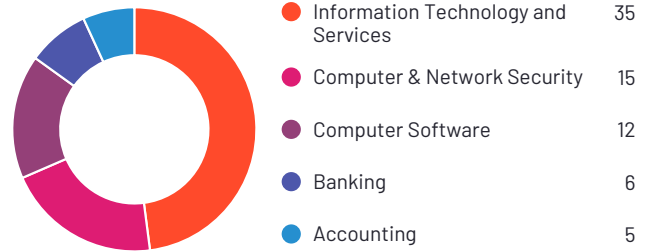


Microsoft Sentinel has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. Microsoft Sentinel has the largest Market Presence among products in Security Orchestration, Automation, and Response (SOAR). 97% of users rated it 4 or 5 stars, 96% of users believe it is headed in the right direction, and users said they would be likely to recommend Microsoft Sentinel at a rate of 89%. Microsoft Sentinel is also in the Security Information and Event Management (SIEM) category.

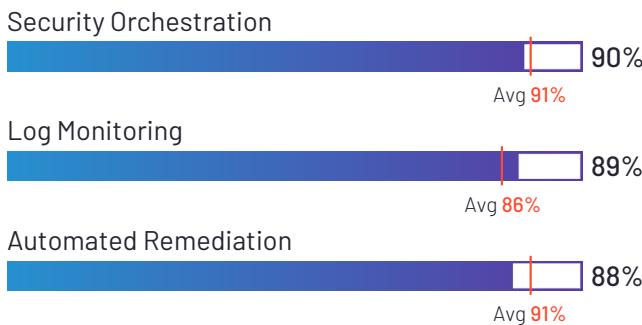
Satisfaction Ratings



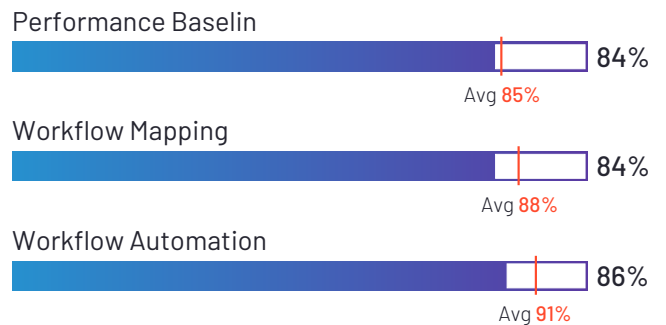
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Microsoft



HQ Location
Redmond,
Washington



Year Founded
1975



Employees (Listed On LinkedIn)
244,409



Company Website
microsoft.com



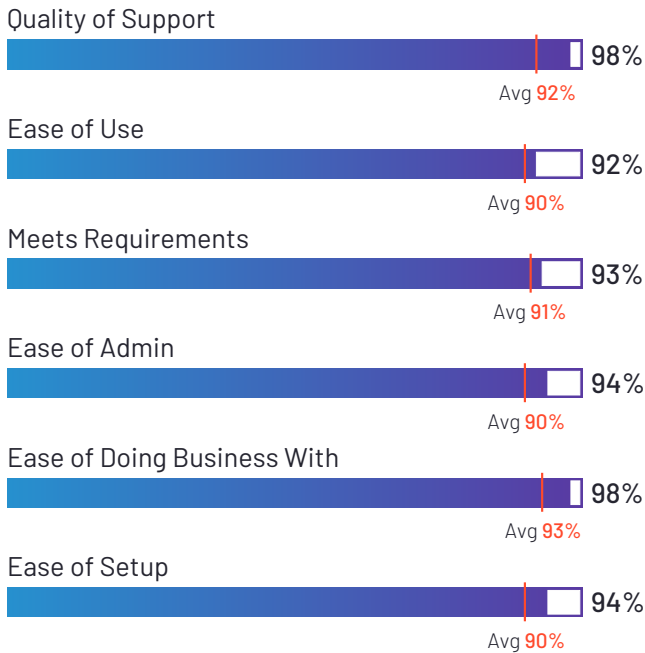
Tines

4.8 ★★★★★ (230)

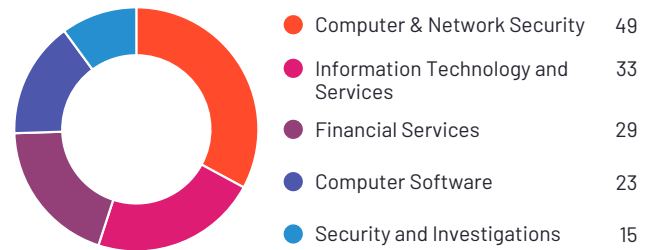


Tines has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 100% of users rated it 4 or 5 stars, 98% of users believe it is headed in the right direction, and users said they would be likely to recommend Tines at a rate of 97%. Tines is also in the Other Process Automation, iPaaS, and Incident Response categories.

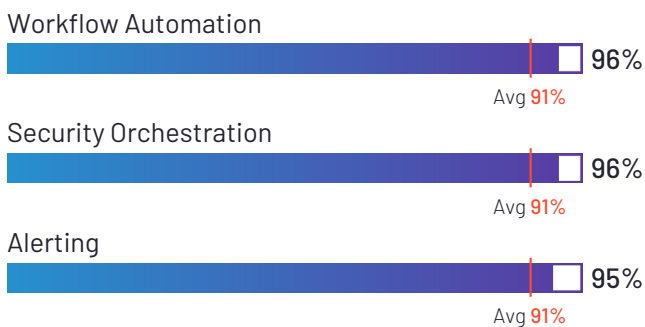
Satisfaction Ratings



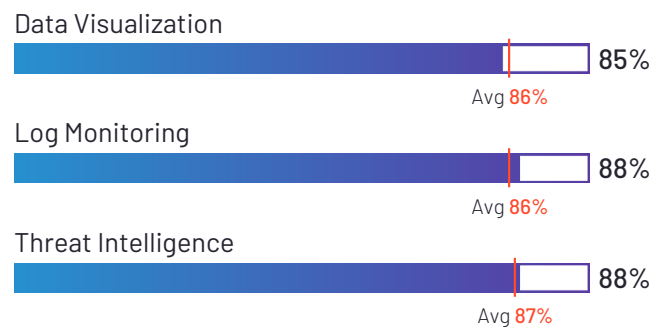
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Tines



HQ Location
Dublin, County Dublin



Year Founded
2018



Employees (Listed
On LinkedIn)
354



Company Website
www.tines.com



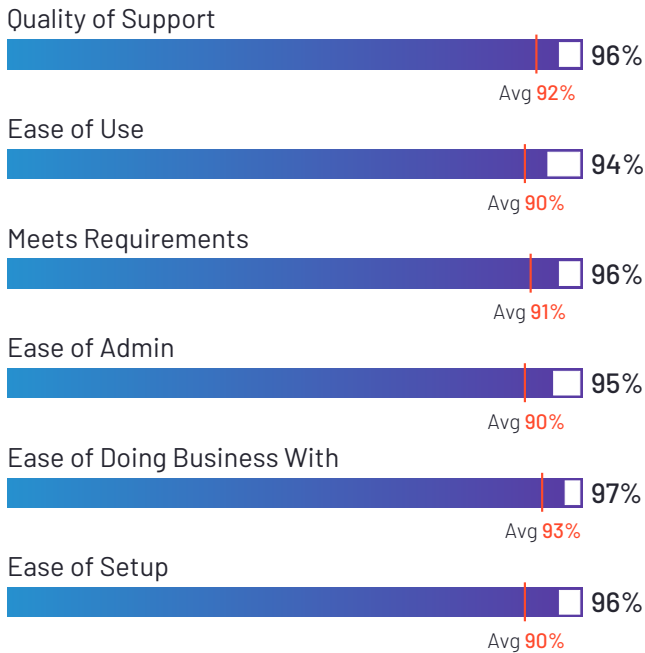
Torq

4.7 ★★★★★ (98)

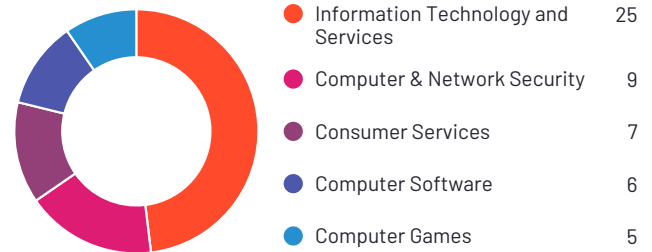


Torq has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Torq at a rate of 95%. Torq is also in the Identity and Access Management (IAM), Incident Response, and Cloud Security Posture Management (CSPM) categories.

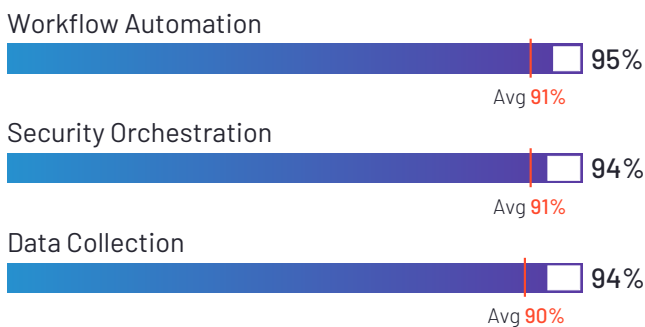
Satisfaction Ratings



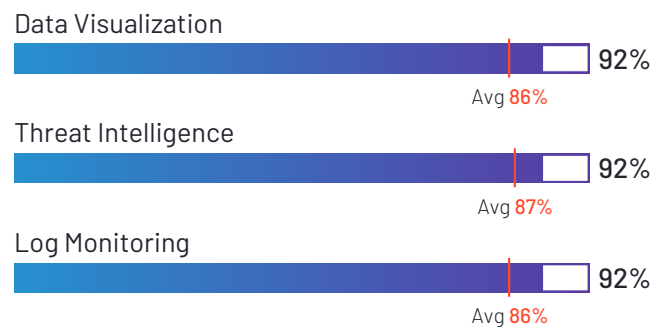
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
torq



HQ Location
New York, US



Year Founded
2020



Employees (Listed
On LinkedIn)
214



Company Website
torq.io



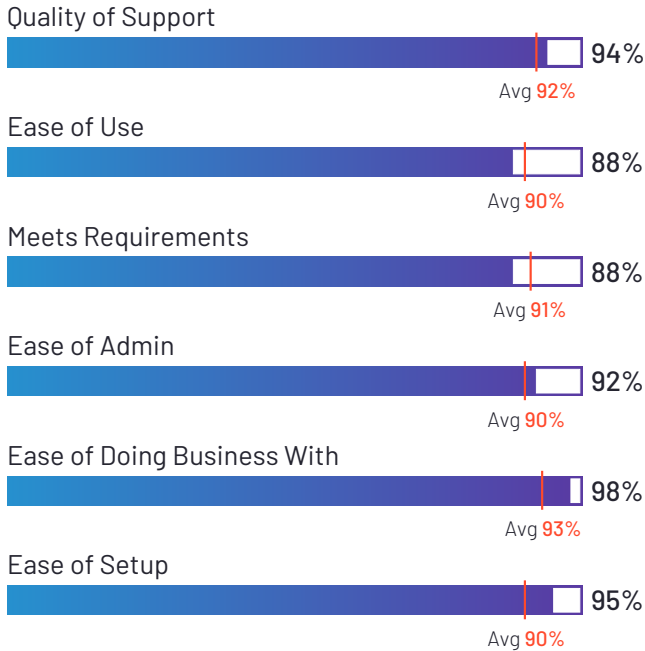
ServiceNow Security Operations

4.4 ★★★★★ (16)

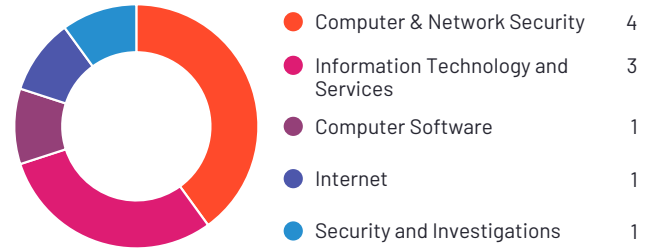


ServiceNow Security Operations has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 100% of users rated it 4 or 5 stars, 83% of users believe it is headed in the right direction, and users said they would be likely to recommend ServiceNow Security Operations at a rate of 91%. ServiceNow Security Operations is also in the Incident Response and Risk-Based Vulnerability Management categories.

Satisfaction Ratings



Top Industries Represented



Ownership
ServiceNow



HQ Location
Santa Clara, CA



Year Founded
2004



Employees (Listed On LinkedIn)
29,061



Company Website
[servicenow.com](https://www.servicenow.com)



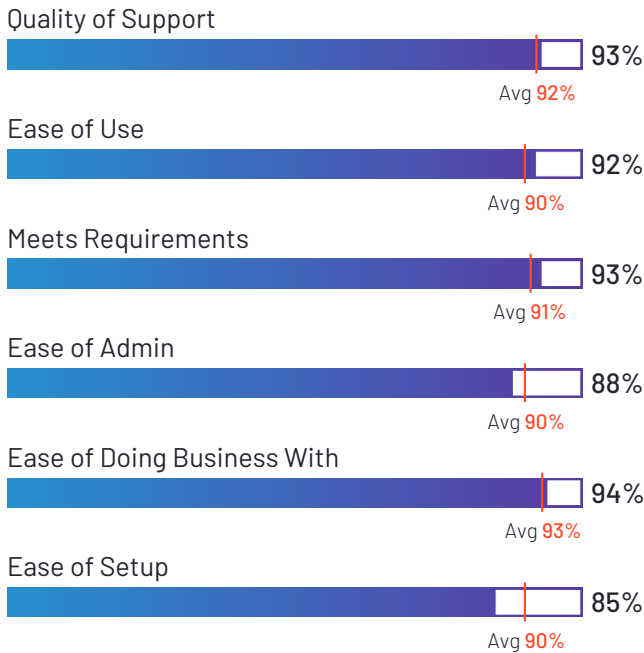
Swimlane

4.6 ★★★★★ (44)

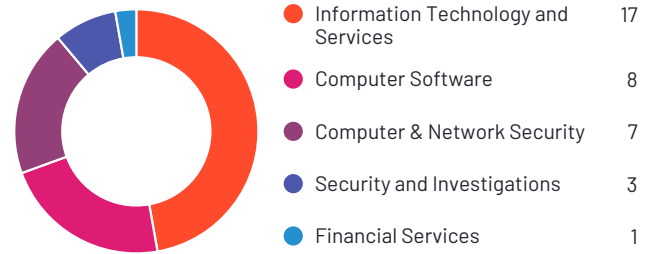


Swimlane has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 100% of users rated it 4 or 5 stars, 92% of users believe it is headed in the right direction, and users said they would be likely to recommend Swimlane at a rate of 93%. Swimlane is also in the Incident Response category.

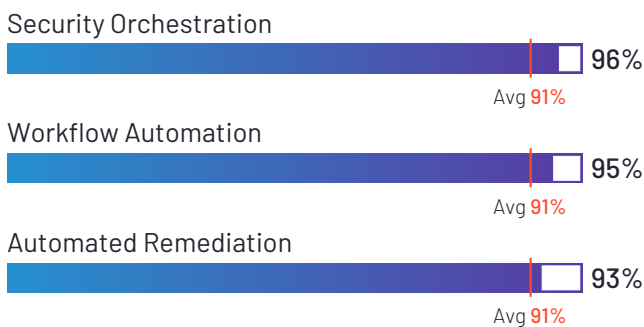
Satisfaction Ratings



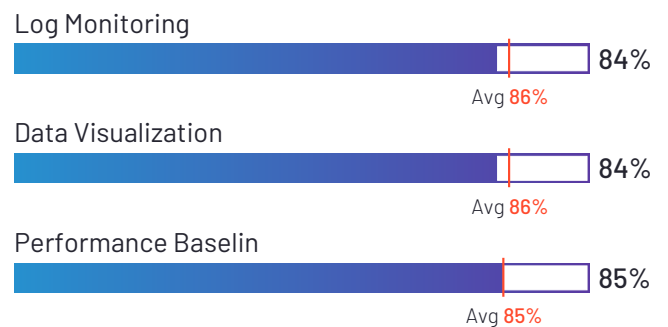
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Swimlane



HQ Location
Boulder, US



Year Founded
2014



Employees (Listed On LinkedIn)
257



Company Website
swimlane.com



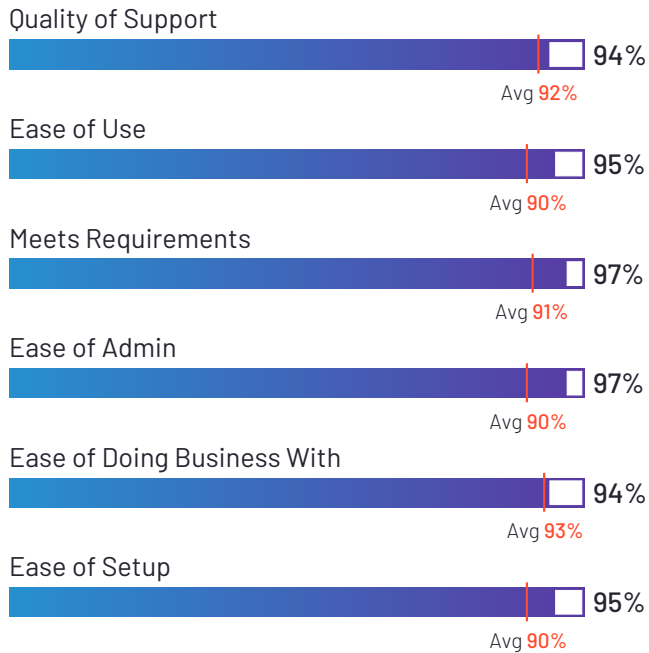
Barracuda Incident Response

4.6 ★★★★★ (17)

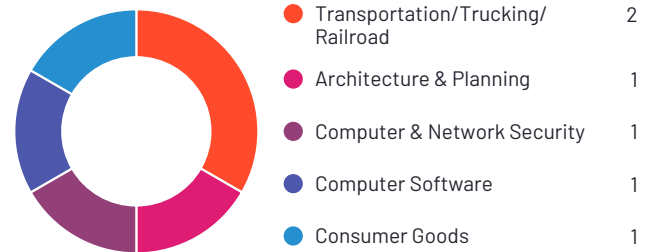


Barracuda Incident Response has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Barracuda Incident Response at a rate of 91%. Barracuda Incident Response is also in the Incident Response category.

Satisfaction Ratings



Top Industries Represented



Ownership
Barracuda



HQ Location
Campbell, CA



Year Founded
2002



Employees (Listed On LinkedIn)
2,139



Company Website
barracuda.com



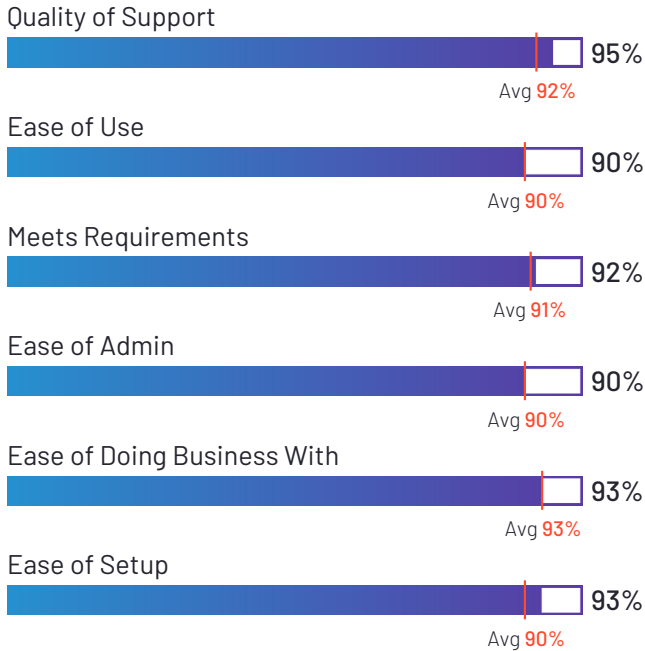
Logpoint

4.3 ★★★★★ (88)

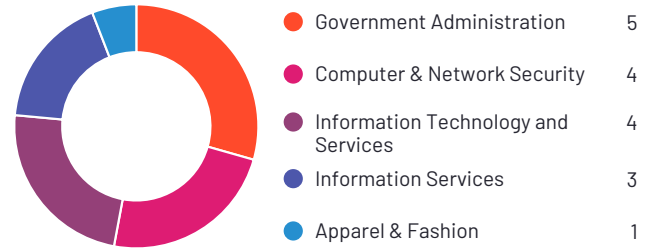


Logpoint has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Logpoint at a rate of 91%. Logpoint is also in the Log Monitoring, Log Analysis, Security Information and Event Management (SIEM), Incident Response, Threat Intelligence, User and Entity Behavior Analytics (UEBA), and SAP Store categories.

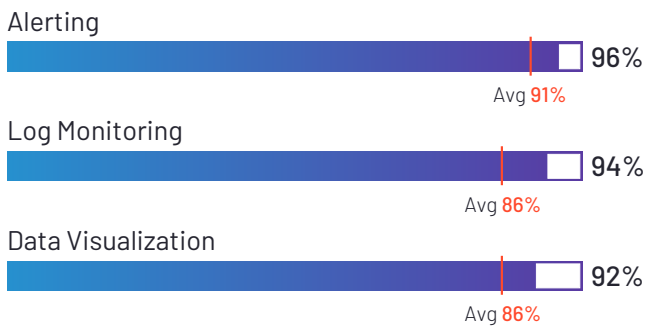
Satisfaction Ratings



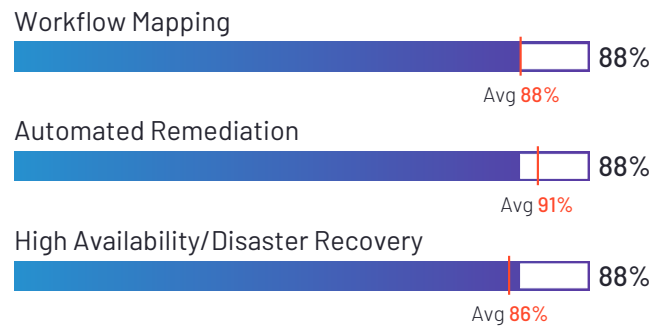
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Logpoint



HQ Location
Copenhagen, Capital Region



Year Founded
2001



Employees (Listed On LinkedIn)
269



Company Website
logpoint.com



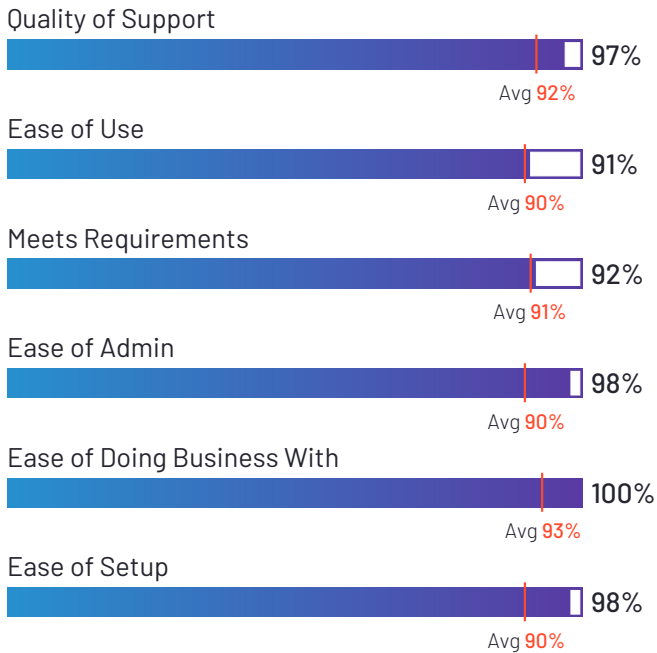
Blink

4.7 ★★★★★ (17)



Blink has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Blink at a rate of 96%. Blink is also in the Workflow Management category.

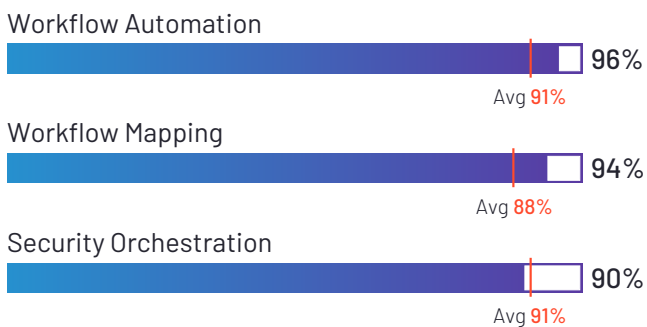
Satisfaction Ratings



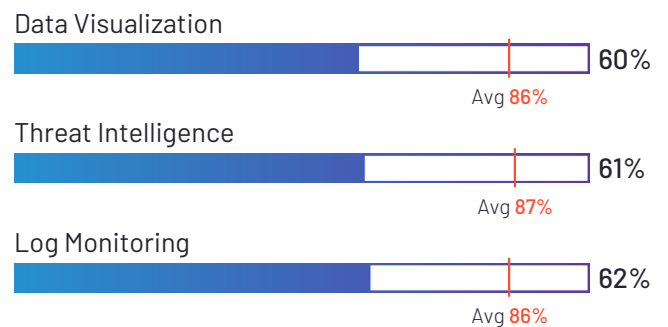
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Blink Ops



HQ Location
Austin, US



Year Founded
2021



Employees (Listed On LinkedIn)
74



Company Website
blinkops.com



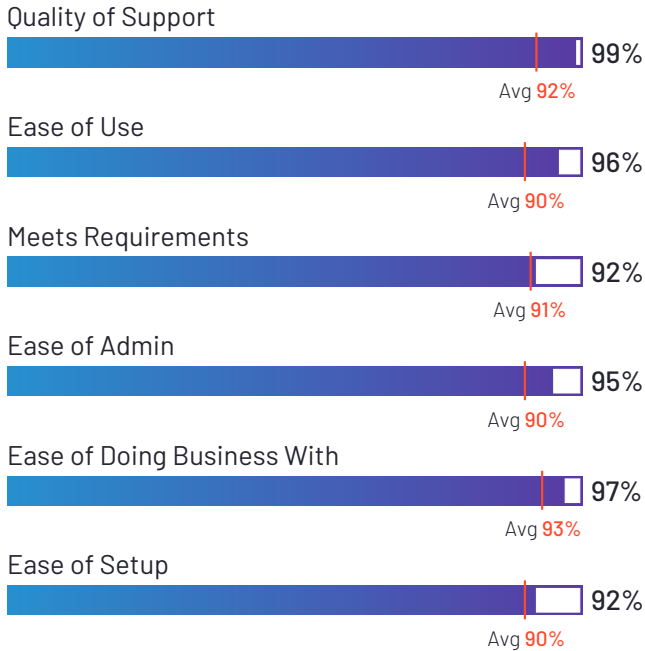
Blumira Automated Detection & Response

4.6 ★★★★★ (107)

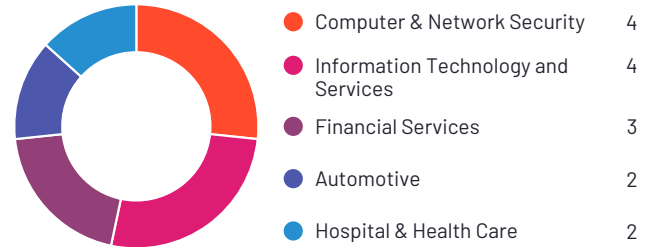


Blumira Automated Detection & Response has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Blumira Automated Detection & Response at a rate of 98%. Blumira Automated Detection & Response is also in the Network Detection and Response (NDR), Cloud Security Monitoring and Analytics, Log Monitoring, Managed Detection and Response (MDR), Intrusion Detection and Prevention Systems (IDPS), Cloud Infrastructure Monitoring, Incident Response, Security Information and Event Management (SIEM), and Extended Detection and Response (XDR) Platforms categories.

Satisfaction Ratings



Top Industries Represented



Ownership
Blumira



HQ Location
Ann Arbor, Michigan



Year Founded
2018



Employees (Listed On LinkedIn)
80



Company Website
blumira.com



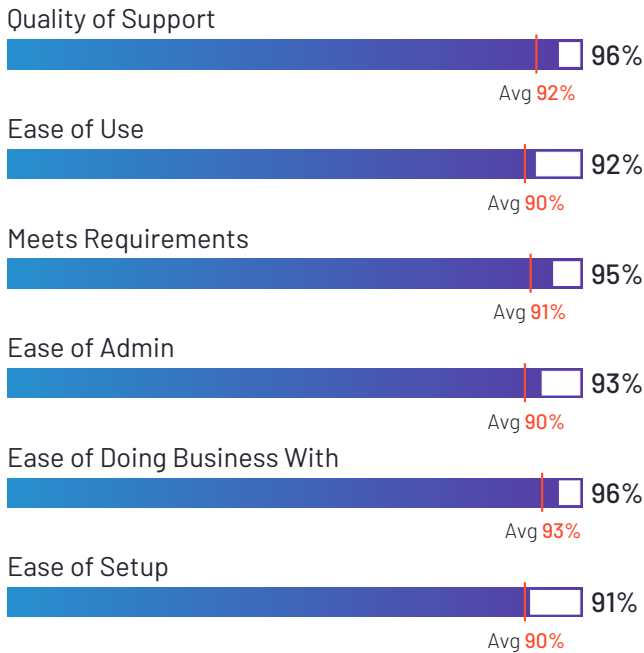
CrowdSec

4.7 ★★★★★ (87)

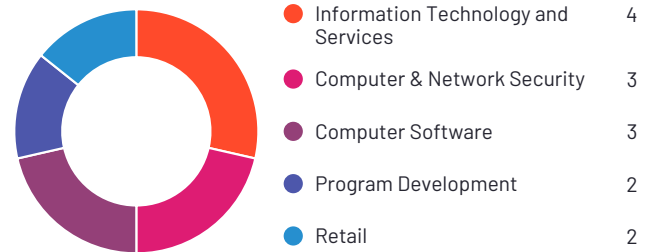


CrowdSec has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 97% of users rated it 4 or 5 stars, 93% of users believe it is headed in the right direction, and users said they would be likely to recommend CrowdSec at a rate of 94%. CrowdSec is also in the Intrusion Detection and Prevention Systems (IDPS), Container Security, Endpoint Detection & Response (EDR), Threat Intelligence, and Firewall Software categories.

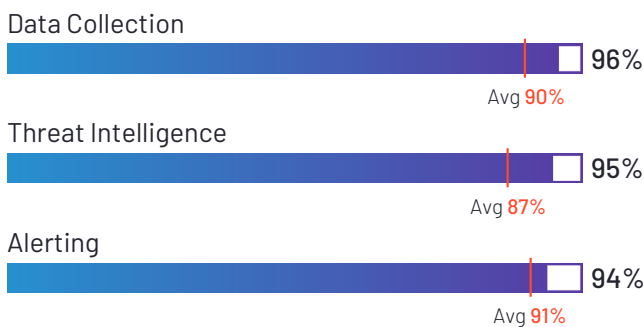
Satisfaction Ratings



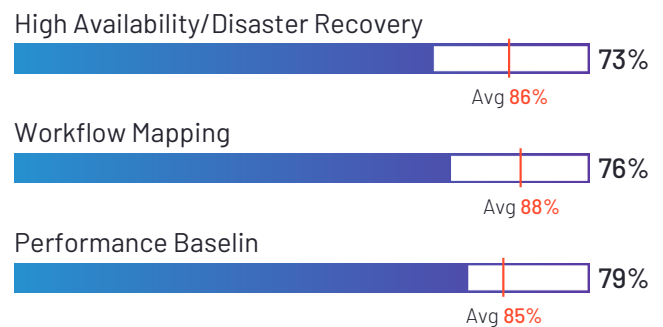
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
CrowdSec



HQ Location
Paris, FR



Year Founded
2020



Employees (Listed
On LinkedIn)
41



Company Website
crowdsec.net



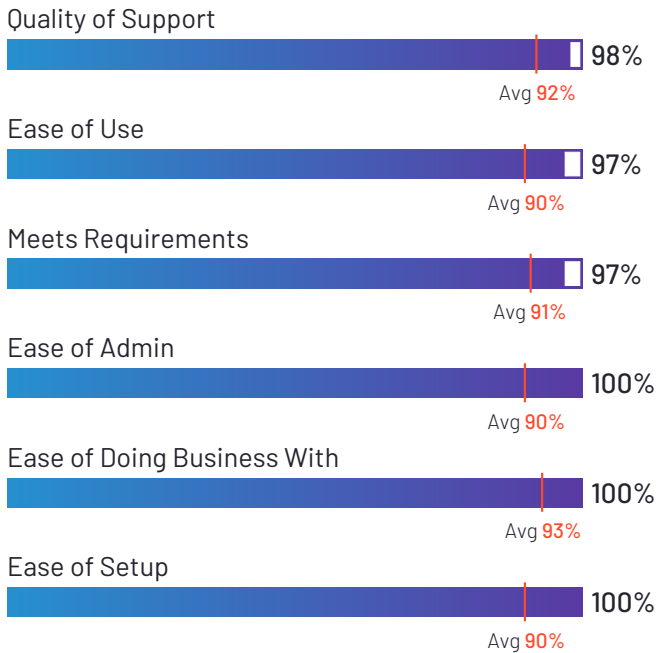
SIRP

4.7 ★★★★★ (27)

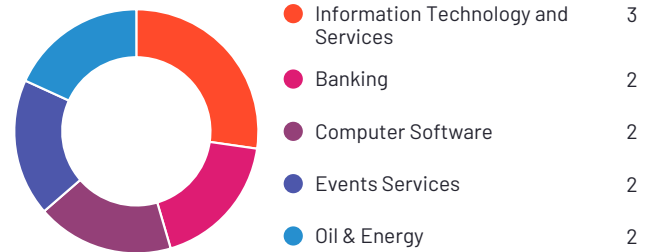


SIRP has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 95% of users rated it 4 or 5 stars, 89% of users believe it is headed in the right direction, and users said they would be likely to recommend SIRP at a rate of 94%. SIRP is also in the Incident Response and Threat Intelligence categories.

Satisfaction Ratings



Top Industries Represented



Ownership
SIRP



HQ Location
London



Year Founded
2017



Employees (Listed On LinkedIn)
28



Company Website
www.sirp.io



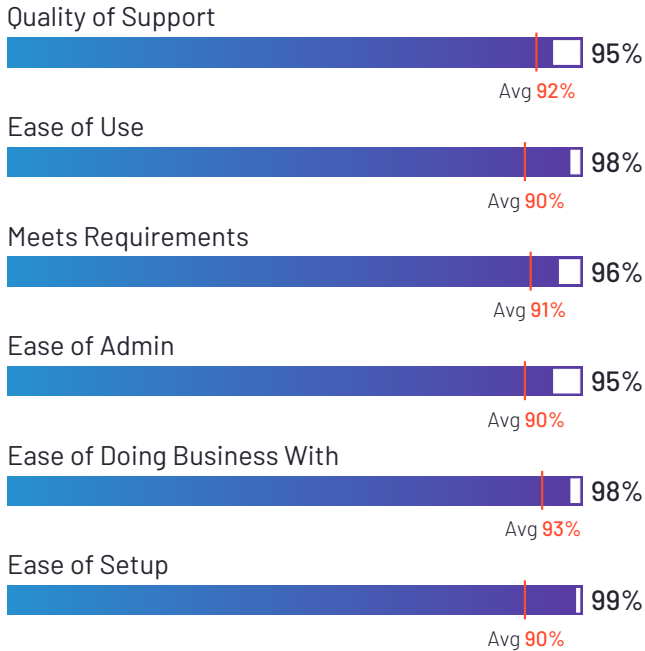
Shuffle

4.8 ★★★★★ (15)

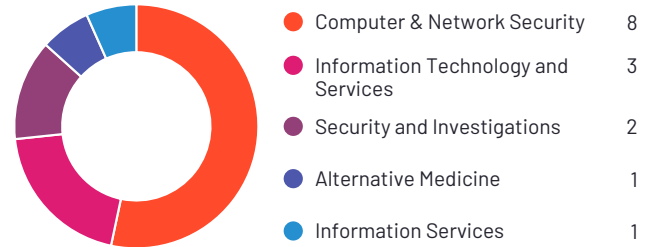


Shuffle has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 93% of users believe it is headed in the right direction, and users said they would be likely to recommend Shuffle at a rate of 96%.

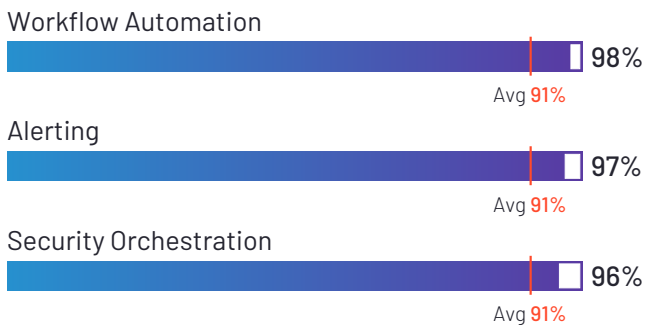
Satisfaction Ratings



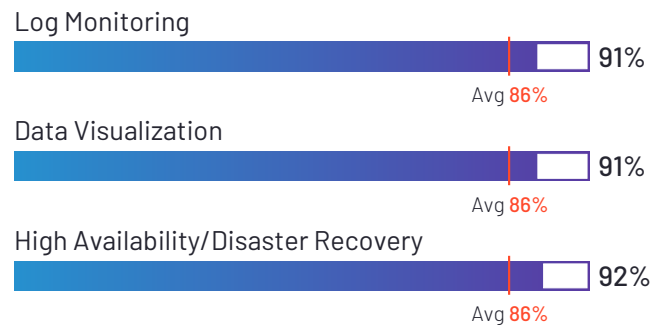
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Shuffle AS



HQ Location
San Francisco, US



Employees (Listed On LinkedIn)
10



Company Website
shuffler.io

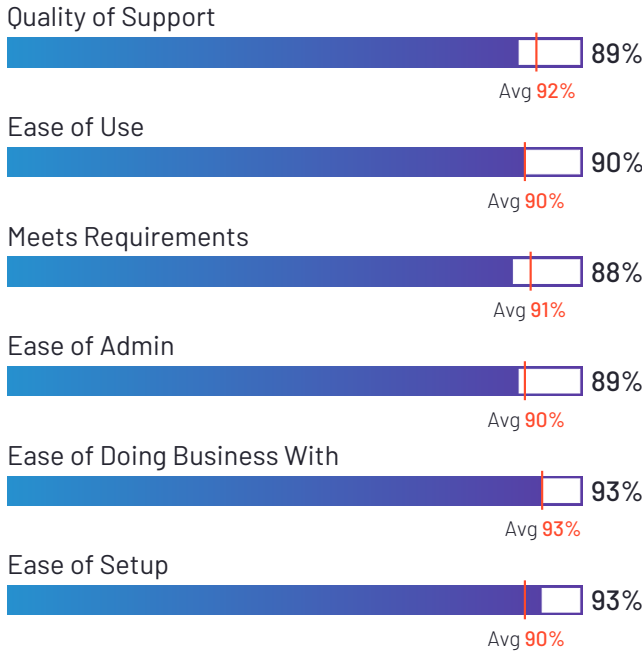


Palo Alto Networks Cortex XSOAR

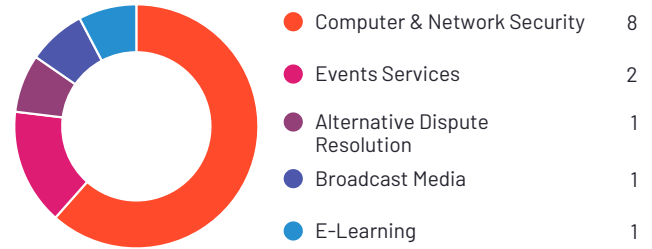
4.5 ★★★★★ (18)

Palo Alto Networks Cortex XSOAR has been named a Contender product based on having a relatively low customer Satisfaction score and large Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 4 or 5 stars, 92% of users believe it is headed in the right direction, and users said they would be likely to recommend Palo Alto Networks Cortex XSOAR at a rate of 90%.

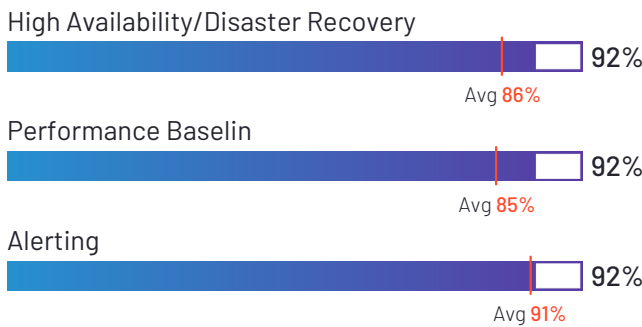
Satisfaction Ratings



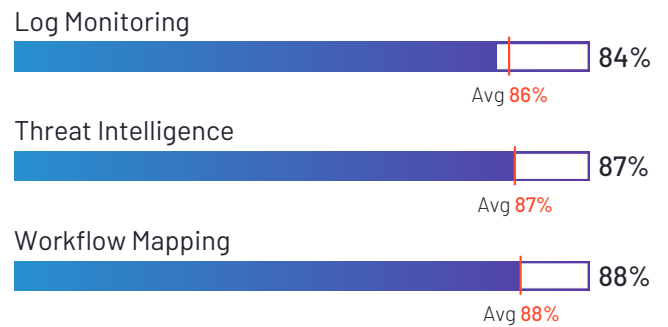
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Palo Alto Networks



HQ Location
Santa Clara, CA



Year Founded
2005



Employees (Listed On LinkedIn)
16,448



Company Website
paloaltonetworks.com

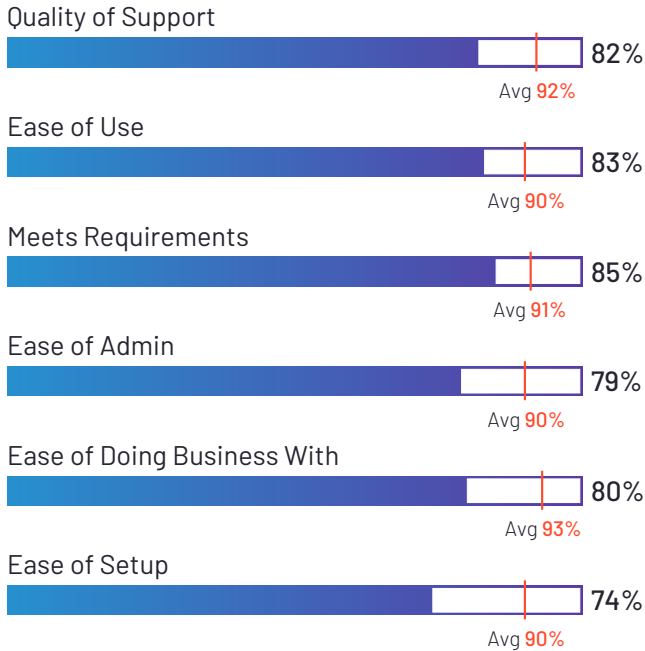


Google Security Operations

4.4 ★★★★★ (36)

Google Security Operations has been named a Contender product based on having a relatively low customer Satisfaction score and large Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 92% of users rated it 4 or 5 stars, 91% of users believe it is headed in the right direction, and users said they would be likely to recommend Google Security Operations at a rate of 87%.

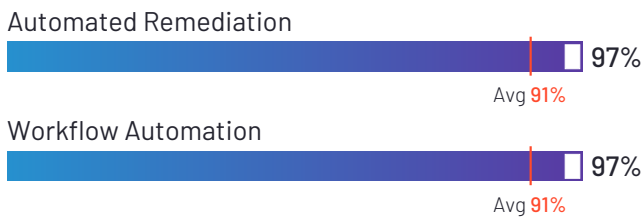
Satisfaction Ratings



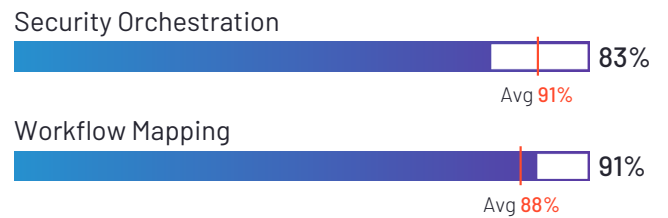
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Google



HQ Location
Mountain View, CA



Year Founded
1998



Employees (Listed On LinkedIn)
302,228



Company Website
cloud.google.com

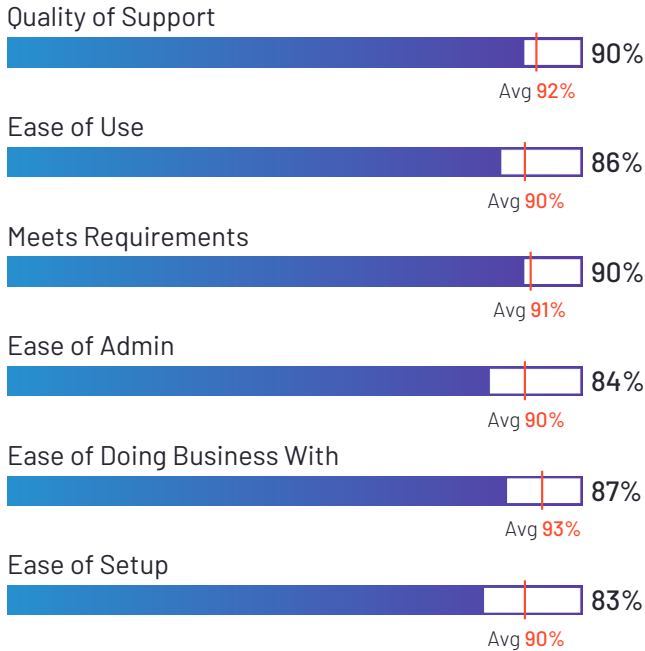
splunk>

Splunk SOAR (Security Orchestration, Automation and Response)

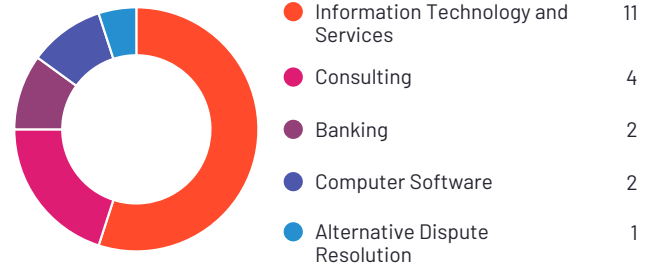
4.4 ★★★★★ (40)

Splunk SOAR (Security Orchestration, Automation and Response) has been named a Contender product based on having a relatively low customer Satisfaction score and large Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 97% of users rated it 4 or 5 stars, 93% of users believe it is headed in the right direction, and users said they would be likely to recommend Splunk SOAR (Security Orchestration, Automation and Response) at a rate of 90%. Splunk SOAR (Security Orchestration, Automation and Response) is also in the Incident Response category.

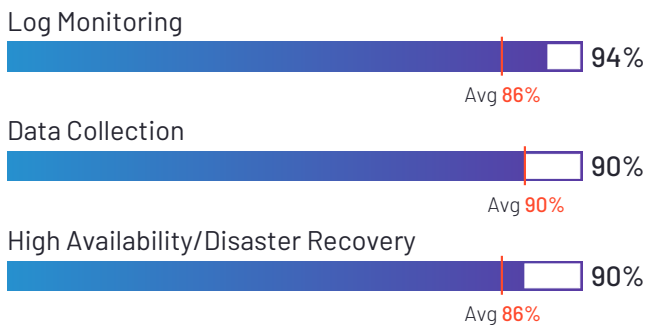
Satisfaction Ratings



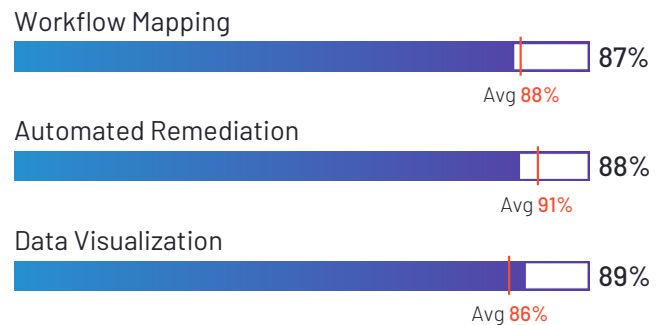
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Cisco



HQ Location
San Jose, CA



Year Founded
1984



Employees (Listed
On LinkedIn)
98,557



Company Website
www.cisco.com

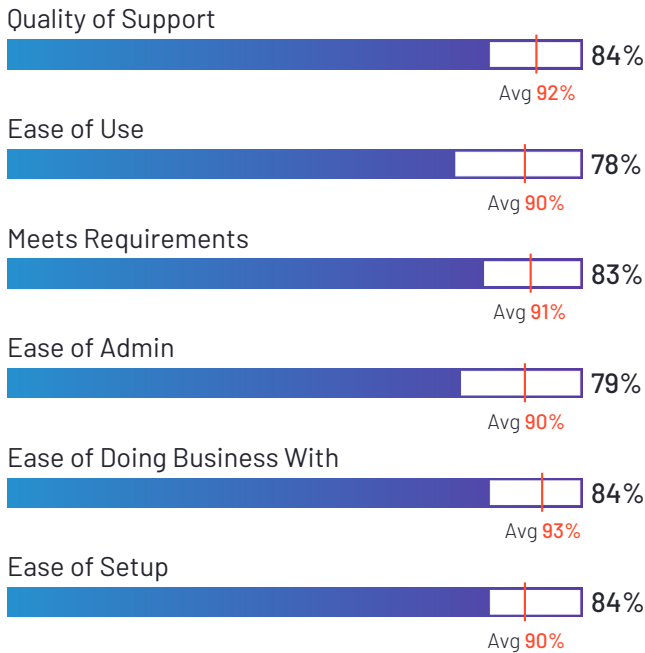


IBM Security QRadar SOAR

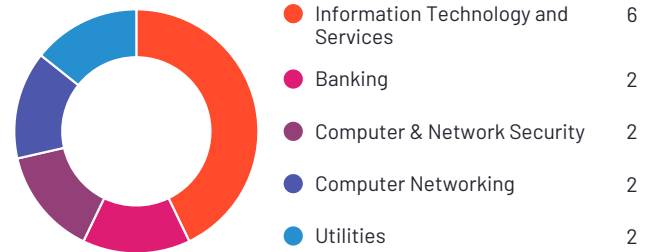
4.1 ★★★★★ (30)

IBM Security QRadar SOAR has been named a Contender product based on having a relatively low customer Satisfaction score and large Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 90% of users rated it 4 or 5 stars, 95% of users believe it is headed in the right direction, and users said they would be likely to recommend IBM Security QRadar SOAR at a rate of 84%. IBM Security QRadar SOAR is also in the ServiceNow Store Apps, Data Breach Notification, and Incident Response categories.

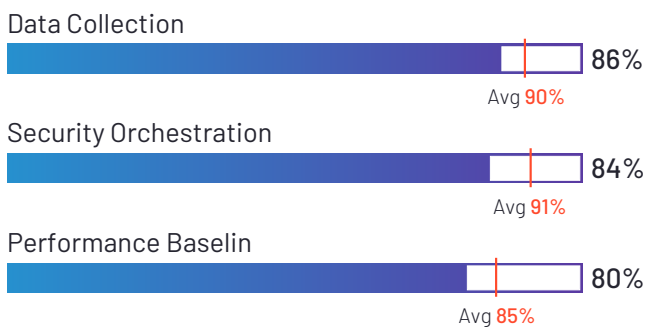
Satisfaction Ratings



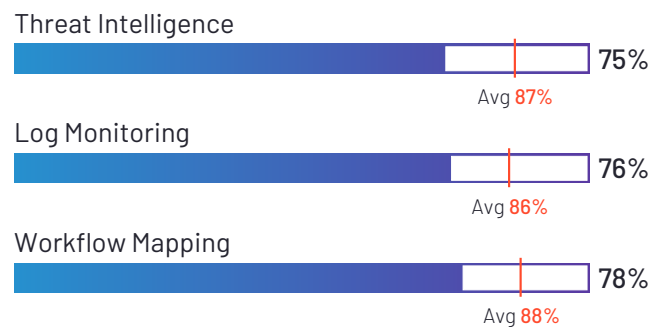
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
IBM



HQ Location
Armonk, NY



Year Founded
1911



Employees (Listed
On LinkedIn)
307,251



Company Website
www.ibm.com

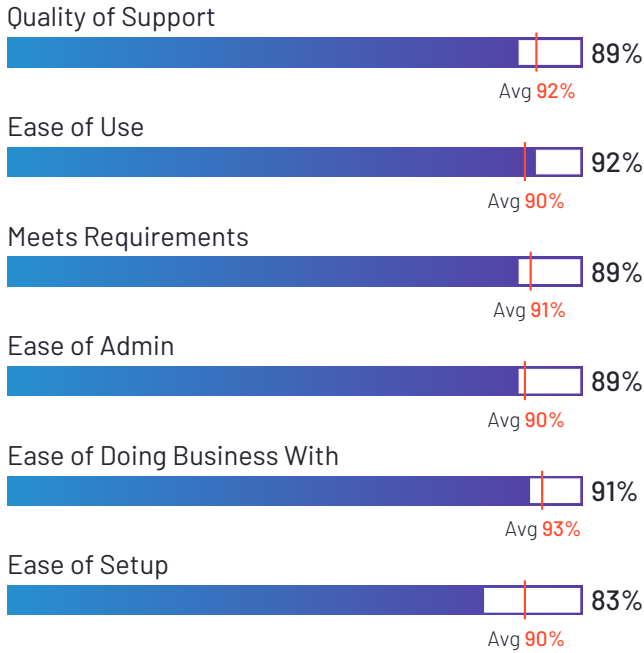


Demisto

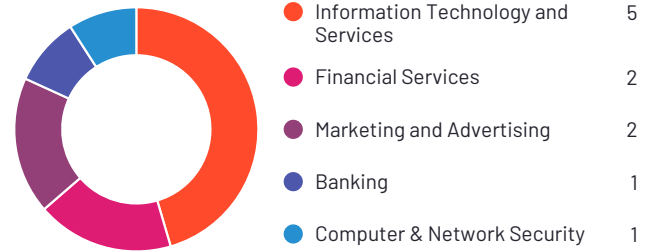
4.5 ★★★★★ (15)

Demisto has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 87% of users rated it 4 or 5 stars, 92% of users believe it is headed in the right direction, and users said they would be likely to recommend Demisto at a rate of 90%. Demisto is also in the Incident Management category.

Satisfaction Ratings



Top Industries Represented



Ownership
Palo Alto Networks



HQ Location
Santa Clara, CA



Year Founded
2005



Employees (Listed On LinkedIn)
16,448



Company Website
paloaltonetworks.com

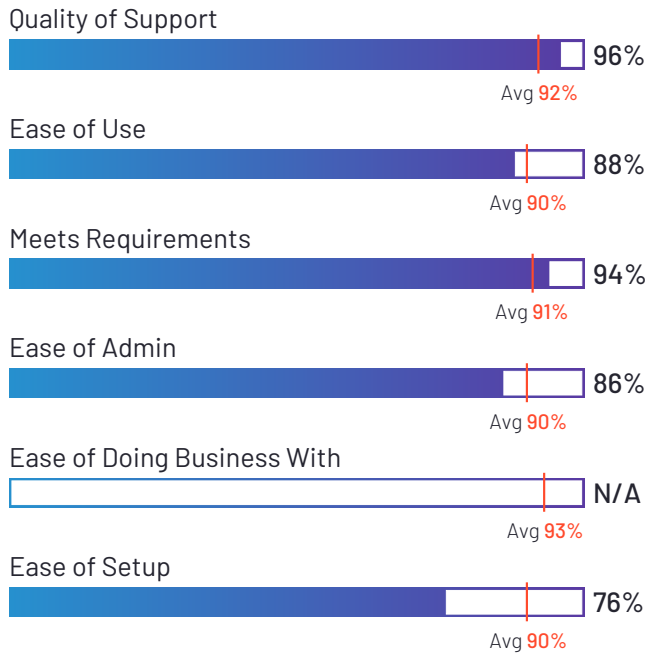


n8n

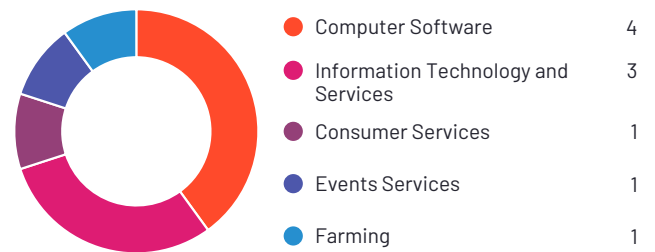
4.8 ★★★★★ (27)

n8n has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend n8n at a rate of 97%. n8n is also in the iPaaS category.

Satisfaction Ratings



Top Industries Represented



*N/A is displayed when fewer than five responses were received for the question.

<p>Ownership n8n GmbH</p>	<p>HQ Location Berlin, Berlin</p>	<p>Year Founded 2019</p>	<p>Employees (Listed On LinkedIn) 70</p>	<p>Company Website n8n.io</p>
--------------------------------------	--	-------------------------------------	---	---

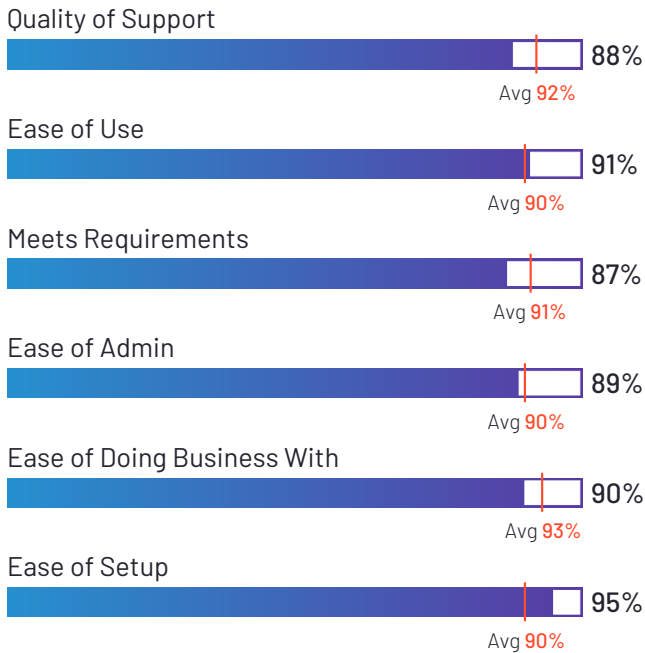


Intezer

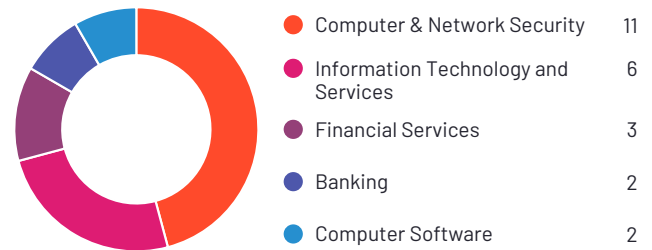
4.5 ★★★★★ (192)

Intezer has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 97% of users rated it 4 or 5 stars, 92% of users believe it is headed in the right direction, and users said they would be likely to recommend Intezer at a rate of 89%. Intezer is also in the Malware Analysis Tools, Network Sandboxing, Threat Intelligence, Managed Detection and Response (MDR), Endpoint Detection & Response (EDR), and Incident Response categories.

Satisfaction Ratings



Top Industries Represented



Ownership
Intezer



HQ Location
New York



Year Founded
2015



Employees (Listed On LinkedIn)
47



Company Website
intezer.com

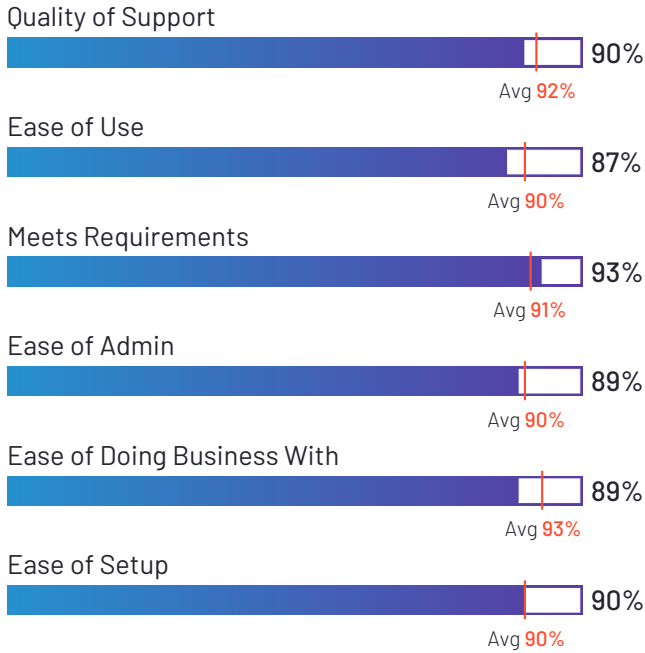


Sumo Logic

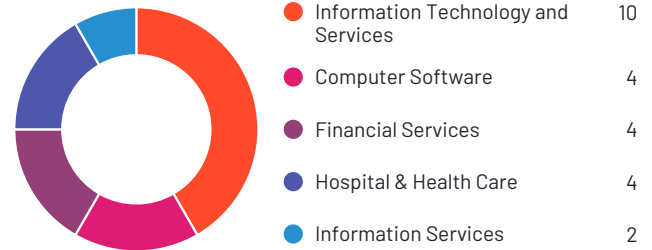
4.3 ★★★★★ (303)

Sumo Logic has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 97% of users rated it 4 or 5 stars, 86% of users believe it is headed in the right direction, and users said they would be likely to recommend Sumo Logic at a rate of 87%. Sumo Logic is also in the Cloud Security Monitoring and Analytics, Log Monitoring, Cloud Infrastructure Monitoring, Container Monitoring, Log Analysis, Incident Response, Security Information and Event Management (SIEM), Application Performance Monitoring (APM), and Observability Solution Suites categories.

Satisfaction Ratings



Top Industries Represented



Ownership
Sumo Logic



HQ Location
Redwood City, CA



Year Founded
2010



Employees (Listed On LinkedIn)
902



Company Website
sumologic.com

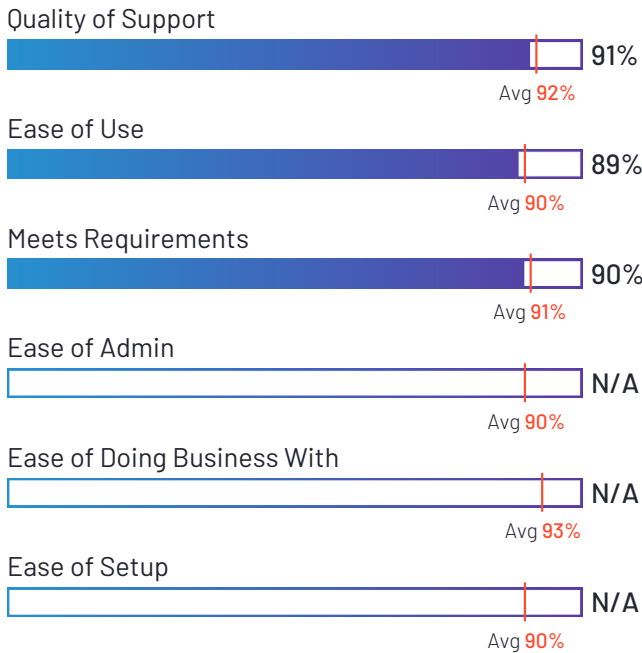


D3 Security

4.2 ★★★★★ (69)

D3 Security has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 95% of users rated it 4 or 5 stars, 95% of users believe it is headed in the right direction, and users said they would be likely to recommend D3 Security at a rate of 87%. D3 Security is also in the Incident Response and Protective Intelligence Platforms categories.

Satisfaction Ratings



Top Industries Represented



*N/A is displayed when fewer than five responses were received for the question.

<p>Ownership D3 Security Management Systems</p>	<p>HQ Location Vancouver, British Columbia</p>	<p>Year Founded 2012</p>	<p>Employees (Listed On LinkedIn) 177</p>	<p>Company Website d3security.com</p>
--	---	-------------------------------------	--	---

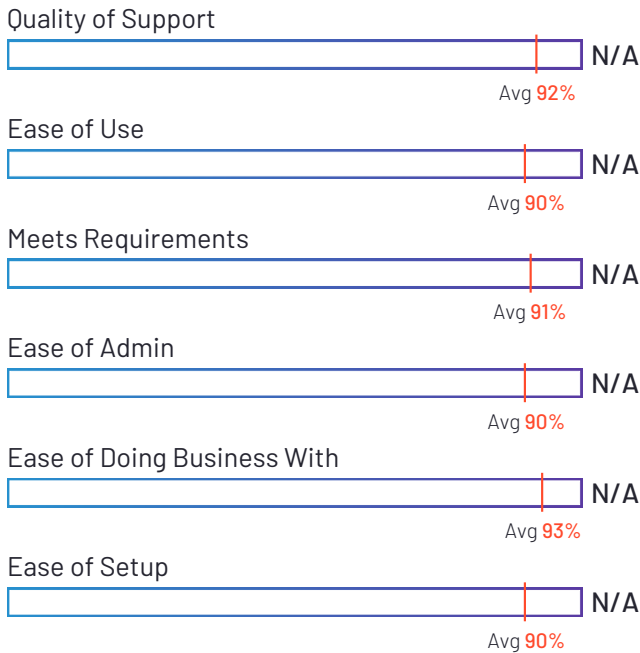


LogicHub

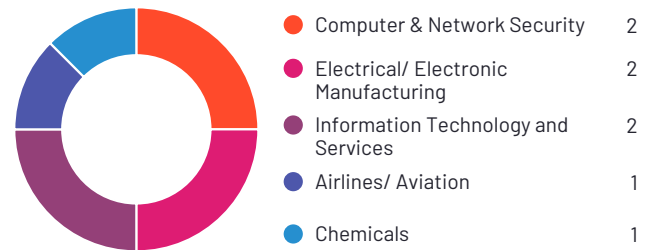
4.7 ★★★★★ (11)

LogicHub has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend LogicHub at a rate of 95%. LogicHub is also in the Incident Response and Managed Detection and Response (MDR) categories.

Satisfaction Ratings



Top Industries Represented



*N/A is displayed when fewer than five responses were received for the question.

<p>Ownership Devo</p>	<p>HQ Location Boston, US</p>	<p>Year Founded 2011</p>	<p>Employees (Listed On LinkedIn) 604</p>	<p>Company Website www.devo.com</p>
----------------------------------	--	-------------------------------------	--	--

Satisfaction Ratings for Security Orchestration, Automation, and Response (SOAR)

G2 reviewers rated software sellers ability to satisfy their needs as shown in the table below.

	Satisfaction		Satisfaction by Category						Net Promoter Score (NPS)
	Likelihood to Recommend	Product Going in Right Direction?	Meets Requirements	Ease of Admin	Ease of Doing Business With	Quality of Support	Ease of Setup	Ease of Use	
KnowBe4 PhishER/PhishER Plus	92%	94%	93%	92%	96%	94%	89%	91%	78
Microsoft Sentinel	89%	96%	89%	85%	91%	86%	86%	87%	65
Tines	97%	98%	93%	94%	98%	98%	94%	92%	93
Torq	95%	100%	96%	95%	97%	96%	96%	94%	94
ServiceNow Security Operations	91%	83%	88%	92%	98%	94%	95%	88%	70
Swimlane	93%	92%	93%	88%	94%	93%	85%	92%	82
Barracuda Incident Response	91%	100%	97%	97%	94%	94%	95%	95%	81
Logpoint	91%	100%	92%	90%	93%	95%	93%	90%	67
Blink	96%	100%	92%	98%	100%	97%	98%	91%	90
Blumira Automated Detection & Response	98%	100%	92%	95%	97%	99%	92%	96%	95
CrowdSec	94%	93%	95%	93%	96%	96%	91%	92%	86
SIRP	94%	89%	97%	100%	100%	98%	100%	97%	78
Shuffle	96%	93%	96%	95%	98%	95%	99%	98%	93
Palo Alto Networks Cortex XSOAR	90%	92%	88%	89%	93%	89%	93%	90%	72
Google Security Operations	87%	91%	85%	79%	80%	82%	74%	83%	57
Splunk SOAR (Security Orchestration, Automation and Response)	90%	93%	90%	84%	87%	90%	83%	86%	68
IBM Security QRadar SOAR	84%	95%	83%	79%	84%	84%	84%	78%	47

(Satisfaction Ratings for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when fewer than five responses were received for the question.

**Net Promoter Score ranges from -100 to +100

Satisfaction Ratings for Security Orchestration, Automation, and Response (SOAR)(continued)

G2 reviewers rated software sellers ability to satisfy their needs as shown in the table below.

	Satisfaction		Satisfaction by Category						Net Promoter Score (NPS)
	Likelihood to Recommend	Product Going in Right Direction?	Meets Requirements	Ease of Admin	Ease of Doing Business With	Quality of Support	Ease of Setup	Ease of Use	
Demisto	90%	92%	89%	89%	91%	89%	83%	92%	66
n8n	97%	100%	94%	86%	N/A	96%	76%	88%	93
Intezer	89%	92%	87%	89%	90%	88%	95%	91%	68
Sumo Logic	87%	86%	93%	89%	89%	90%	90%	87%	62
D3 Security	87%	95%	90%	N/A	N/A	91%	N/A	89%	54
LogicHub	95%	N/A	N/A	N/A	N/A	N/A	N/A	N/A	100
Average	92%	94%	91%	90%	93%	92%	90%	90%	76

*N/A is displayed when fewer than five responses were received for the question.

**Net Promoter Score ranges from -100 to +100

Feature Comparison for Security Orchestration, Automation, and Response (SOAR)

G2 users have evaluated the following products by feature. Feature ratings are representative of reviewers overall satisfaction with each feature and do not necessarily take into account the breadth of individual product features. The results are shown below.

Automation

	Workflow Mapping	Workflow Automation	Automated Remediation	Log Monitoring
KnowBe4 PhishER/PhishER Plus	86%	89%	90%	88%
Microsoft Sentinel	84%	86%	88%	89%
Tines	94%	96%	94%	88%
Torq	92%	95%	94%	92%
ServiceNow Security Operations	N/A	N/A	N/A	N/A
Swimlane	86%	95%	93%	84%
Barracuda Incident Response	N/A	N/A	N/A	N/A
Logpoint	88%	90%	88%	94%
Blink	94%	96%	90%	62%
Blumira Automated Detection & Response		N/A	N/A	N/A
CrowdSec	76%	81%	92%	94%
SIRP	N/A	N/A	N/A	N/A
Shuffle	95%	98%	96%	91%
Palo Alto Networks Cortex XSOAR	88%	88%	90%	84%
Google Security Operations	91%	97%	97%	N/A
Splunk SOAR (Security Orchestration, Automation and Response)	87%	89%	88%	94%
IBM Security QRadar SOAR	78%	79%	79%	76%

(Feature Comparison for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when fewer than five responses were received for the question.

**A blank box indicates that a seller has selected that they do not offer that feature.

Feature Comparison for Security Orchestration, Automation, and Response (SOAR)(continued)

G2 users have evaluated the following products by feature. Feature ratings are representative of reviewers overall satisfaction with each feature and do not necessarily take into account the breadth of individual product features. The results are shown below.

Automation

	Workflow Mapping	Workflow Automation	Automated Remediation	Log Monitoring
Demisto	N/A	N/A	N/A	N/A
n8n	N/A	N/A	N/A	N/A
Intezer		N/A	N/A	
Sumo Logic	N/A	N/A	N/A	N/A
D3 Security	N/A	N/A	N/A	N/A
LogicHub	N/A	N/A	N/A	N/A
Average	88%	91%	91%	86%

(Feature Comparison for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when fewer than five responses were received for the question.

**A blank box indicates that a seller has selected that they do not offer that feature.

Feature Comparison for Security Orchestration, Automation, and Response (SOAR)(continued)

G2 users have evaluated the following products by feature. Feature ratings are representative of reviewers overall satisfaction with each feature and do not necessarily take into account the breadth of individual product features. The results are shown below.

Orchestration

	Security Orchestration	Data Collection	Threat Intelligence	Data Visualization
KnowBe4 PhishER/PhishER Plus	89%	89%	90%	88%
Microsoft Sentinel	90%	88%	87%	86%
Tines	96%	91%	88%	85%
Torq	94%	94%	92%	92%
ServiceNow Security Operations	N/A	N/A	N/A	N/A
Swimlane	96%	87%	90%	84%
Barracuda Incident Response	N/A	N/A	N/A	N/A
Logpoint	92%	91%	90%	92%
Blink	90%	81%	61%	60%
Blumira Automated Detection & Response	N/A	N/A	N/A	N/A
CrowdSec	87%	96%	95%	90%
SIRP	N/A	N/A	N/A	N/A
Shuffle	96%	92%	96%	91%
Palo Alto Networks Cortex XSOAR	92%	90%	87%	92%
Google Security Operations	83%	N/A	N/A	N/A
Splunk SOAR (Security Orchestration, Automation and Response)	90%	90%	90%	89%
IBM Security QRadar SOAR	84%	86%	75%	80%

(Feature Comparison for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when fewer than five responses were received for the question.

**A blank box indicates that a seller has selected that they do not offer that feature.

Feature Comparison for Security Orchestration, Automation, and Response (SOAR)(continued)

G2 users have evaluated the following products by feature. Feature ratings are representative of reviewers overall satisfaction with each feature and do not necessarily take into account the breadth of individual product features. The results are shown below.

Orchestration

	Security Orchestration	Data Collection	Threat Intelligence	Data Visualization
Demisto	N/A	N/A	N/A	N/A
n8n	N/A	N/A	N/A	N/A
Intezer	N/A	N/A	N/A	N/A
Sumo Logic	N/A	N/A	N/A	N/A
D3 Security	N/A	N/A	N/A	N/A
LogicHub	N/A	N/A	N/A	N/A
Average	91%	90%	87%	86%

(Feature Comparison for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when fewer than five responses were received for the question.

**A blank box indicates that a seller has selected that they do not offer that feature.

Feature Comparison for Security Orchestration, Automation, and Response (SOAR)(continued)

G2 users have evaluated the following products by feature. Feature ratings are representative of reviewers overall satisfaction with each feature and do not necessarily take into account the breadth of individual product features. The results are shown below.

Response

	Alerting	Performance Baselin	High Availability/Disaster Recovery
KnowBe4 PhishER/PhishER Plus	90%		86%
Microsoft Sentinel	88%	84%	87%
Tines	95%	89%	90%
Torq	94%	93%	93%
ServiceNow Security Operations	N/A	N/A	N/A
Swimlane	90%	85%	88%
Barracuda Incident Response	N/A	N/A	N/A
Logpoint	96%	89%	88%
Blink	84%	63%	76%
Blumira Automated Detection & Response	N/A	N/A	N/A
CrowdSec	94%	79%	73%
SIRP	N/A	N/A	N/A
Shuffle	97%	93%	92%
Palo Alto Networks Cortex XSOAR	92%	92%	92%
Google Security Operations	94%	N/A	N/A
Splunk SOAR (Security Orchestration, Automation and Response)	90%	90%	90%
IBM Security QRadar SOAR	80%	80%	79%

(Feature Comparison for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when fewer than five responses were received for the question.

**A blank box indicates that a seller has selected that they do not offer that feature.

Feature Comparison for Security Orchestration, Automation, and Response (SOAR)(continued)

G2 users have evaluated the following products by feature. Feature ratings are representative of reviewers overall satisfaction with each feature and do not necessarily take into account the breadth of individual product features. The results are shown below.

Response

	Alerting	Performance Baselin	High Availability/Disaster Recovery
Demisto	N/A	N/A	N/A
n8n	N/A	N/A	N/A
Intezer	N/A		N/A
Sumo Logic	N/A	N/A	N/A
D3 Security	N/A	N/A	N/A
LogicHub	N/A	N/A	N/A
Average	91%	85%	86%

*N/A is displayed when fewer than five responses were received for the question.

**A blank box indicates that a seller has selected that they do not offer that feature.

Additional Data for Security Orchestration, Automation, and Response (SOAR)

The table below includes a breakdown of the customer segments for each product, as represented by G2 reviewers.

Customers by Size

	Small Business (50 or fewer emp.)	Mid-Market (51-1000 emp.)	Enterprise (>1000 emp.)
KnowBe4 PhishER/PhishER Plus	12%	77%	11%
Microsoft Sentinel	22%	33%	44%
Tines	22%	37%	41%
Torq	33%	38%	29%
ServiceNow Security Operations	30%	30%	40%
Swimlane	33%	48%	20%
Barracuda Incident Response	27%	55%	18%
Logpoint	29%	50%	21%
Blink	18%	55%	27%
Blumira Automated Detection & Response	13%	70%	17%
CrowdSec	72%	14%	14%
SIRP	42%	26%	32%
Shuffle	33%	67%	0%
Palo Alto Networks Cortex XSOAR	22%	22%	56%
Google Security Operations	8%	27%	65%
Splunk SOAR (Security Orchestration, Automation and Response)	28%	38%	34%
IBM Security QRadar SOAR	10%	14%	76%

(Additional Data for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when data is not publicly available.

Additional Data for Security Orchestration, Automation, and Response (SOAR)(continued)

The table below includes a breakdown of the customer segments for each product, as represented by G2 reviewers.

Customers by Size

	Small Business (50 or fewer emp.)	Mid-Market (51-1000 emp.)	Enterprise (>1000 emp.)
Demisto	40%	40%	20%
n8n	73%	27%	0%
Intezer	42%	34%	24%
Sumo Logic	11%	46%	43%
D3 Security	26%	29%	45%
LogicHub	18%	27%	55%
Average	29%	39%	32%

(Additional Data for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when data is not publicly available.

Additional Data for Security Orchestration, Automation, and Response (SOAR)(continued)

The table below highlights implementation and deployment data as indicated in real user reviews on G2.

Implementation

	Deployment		Implementation Time	Implementation Method				Number of Users Purchased	Contract Term
	Cloud	On-Premises	Avg. Months to Go Live	In-House Team	Seller Services Team	Third-Party Consultant	Don't know	Median Number of Users Bought	Avg. Contract Term (Months)
KnowBe4 PhishER/PhishER Plus	82%	18%	1.3	78%	16%	3%	2%	75	25
Microsoft Sentinel	83%	17%	2.7	63%	15%	14%	8%	56	9
Tines	80%	20%	0.9	80%	9%	2%	9%	7	10
Torq	82%	18%	1.4	60%	20%	0%	20%	17	13
ServiceNow Security Operations	33%	67%	N/A	60%	20%	0%	20%	N/A	N/A
Swimlane	47%	53%	5.2	75%	19%	6%	0%	17	16
Barracuda Incident Response	80%	20%	3.3	80%	0%	0%	20%	N/A	N/A
Logpoint	8%	92%	2.0	46%	23%	8%	23%	7	8
Blink	100%	0%	0.8	83%	17%	0%	0%	7	N/A
Blumira Automated Detection & Response	87%	13%	0.4	80%	13%	7%	0%	7	13
CrowdSec	55%	45%	0.4	90%	0%	0%	10%	3	0
SIRP	71%	29%	0.7	N/A	N/A	N/A	N/A	N/A	N/A
Shuffle	100%	0%	0.1	67%	22%	11%	0%	7	10
Palo Alto Networks Cortex XSOAR	33%	67%	2.1	13%	75%	0%	13%	17	26
Google Security Operations	11%	89%	3.7	38%	62%	0%	0%	7	24
Splunk SOAR (Security Orchestration, Automation and Response)	30%	70%	N/A	38%	38%	25%	0%	N/A	N/A
IBM Security QRadar SOAR	50%	50%	3.9	63%	25%	0%	13%	12	19

(Additional Data for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when data is not publicly available.

Additional Data for Security Orchestration, Automation, and Response (SOAR)(continued)

The table below highlights implementation and deployment data as indicated in real user reviews on G2.

Implementation

	Deployment		Implementation Time	Implementation Method				Number of Users Purchased	Contract Term
	Cloud	On-Premises	Avg. Months to Go Live	In-House Team	Seller Services Team	Third-Party Consultant	Don't know	Median Number of Users Bought	Avg. Contract Term (Months)
Demisto	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
n8n	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Intezer	43%	57%	N/A	83%	0%	0%	17%	N/A	N/A
Sumo Logic	75%	25%	1.1	75%	25%	0%	0%	12	N/A
D3 Security	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
LogicHub	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

(Additional Data for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when data is not publicly available.

Additional Data for Security Orchestration, Automation, and Response (SOAR)(continued)

The table below highlights the average user adoption of each product as indicated in real user reviews on G2.

User Adoption and Return on Investment (ROI)

	User Adoption	Payback Period
	Average User Adoption	Estimated ROI (payback period in months)
KnowBe4 PhishER/PhishER Plus	78%	13
Microsoft Sentinel	53%	17
Tines	40%	8
Torq	51%	13
ServiceNow Security Operations	N/A	N/A
Swimlane	63%	19
Barracuda Incident Response	68%	N/A
Logpoint	35%	26
Blink	59%	N/A
Blumira Automated Detection & Response	76%	7
CrowdSec	70%	3
SIRP	N/A	N/A
Shuffle	49%	16
Palo Alto Networks Cortex XSOAR	31%	15
Google Security Operations	54%	32
Splunk SOAR (Security Orchestration, Automation and Response)	N/A	N/A
IBM Security QRadar SOAR	54%	14

(Additional Data for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when data is not publicly available.

Additional Data for Security Orchestration, Automation, and Response (SOAR)(continued)

The table below highlights the average user adoption of each product as indicated in real user reviews on G2.

User Adoption and Return on Investment (ROI)

	User Adoption	Payback Period
	Average User Adoption	Estimated ROI (payback period in months)
Demisto	N/A	N/A
n8n	N/A	N/A
Intezer	N/A	N/A
Sumo Logic	79%	N/A
D3 Security	N/A	N/A
LogicHub	N/A	N/A
Average	57%	15

(Additional Data for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when data is not publicly available.

Additional Data for Security Orchestration, Automation, and Response (SOAR)(continued)

The table below highlights third-party market presence data used to inform the G2's Market Presence Score that highlights each products impact and influence in the category.

Market Presence

	Seller Name	Year Founded	Employees on LinkedIn (Seller)	LinkedIn Followers
KnowBe4 PhishER/PhishER Plus	KnowBe4, Inc.	2010	1,934	275,873
Microsoft Sentinel	Microsoft	1975	244,409	23,897,870
Tines	Tines	2018	354	38,919
Torq	torq	2020	214	17,436
ServiceNow Security Operations	ServiceNow	2004	29,061	1,061,356
Swimlane	Swimlane	2014	257	13,518
Barracuda Incident Response	Barracuda	2002	2,139	66,211
Logpoint	Logpoint	2001	269	25,769
Blink	Blink Ops	2021	74	11,985
Blumira Automated Detection & Response	Blumira	2018	80	6,706
CrowdSec	CrowdSec	2020	41	11,749
SIRP	SIRP	2017	28	2,857
Shuffle	Shuffle AS		10	283
Palo Alto Networks Cortex XSOAR	Palo Alto Networks	2005	16,448	1,320,642
Google Security Operations	Google	1998	302,228	34,631,050
Splunk SOAR (Security Orchestration, Automation and Response)	Cisco	1984	98,557	6,413,048
IBM Security QRadar SOAR	IBM	1911	307,251	16,469,305

(Additional Data for Security Orchestration, Automation, and Response (SOAR) continues on next page)

*N/A is displayed when data is not publicly available.

Additional Data for Security Orchestration, Automation, and Response (SOAR)(continued)

The table below highlights third-party market presence data used to inform the G2's Market Presence Score that highlights each products impact and influence in the category.

Market Presence

	Seller Name	Year Founded	Employees on LinkedIn (Seller)	LinkedIn Followers
Demisto	Palo Alto Networks	2005	16,448	1,320,642
n8n	n8n GmbH	2019	70	35,533
Intezer	Intezer	2015	47	7,547
Sumo Logic	Sumo Logic	2010	902	155,955
D3 Security	D3 Security Management Systems	2012	177	17,995
LogicHub	Devo	2011	604	35,738

*N/A is displayed when data is not publicly available.