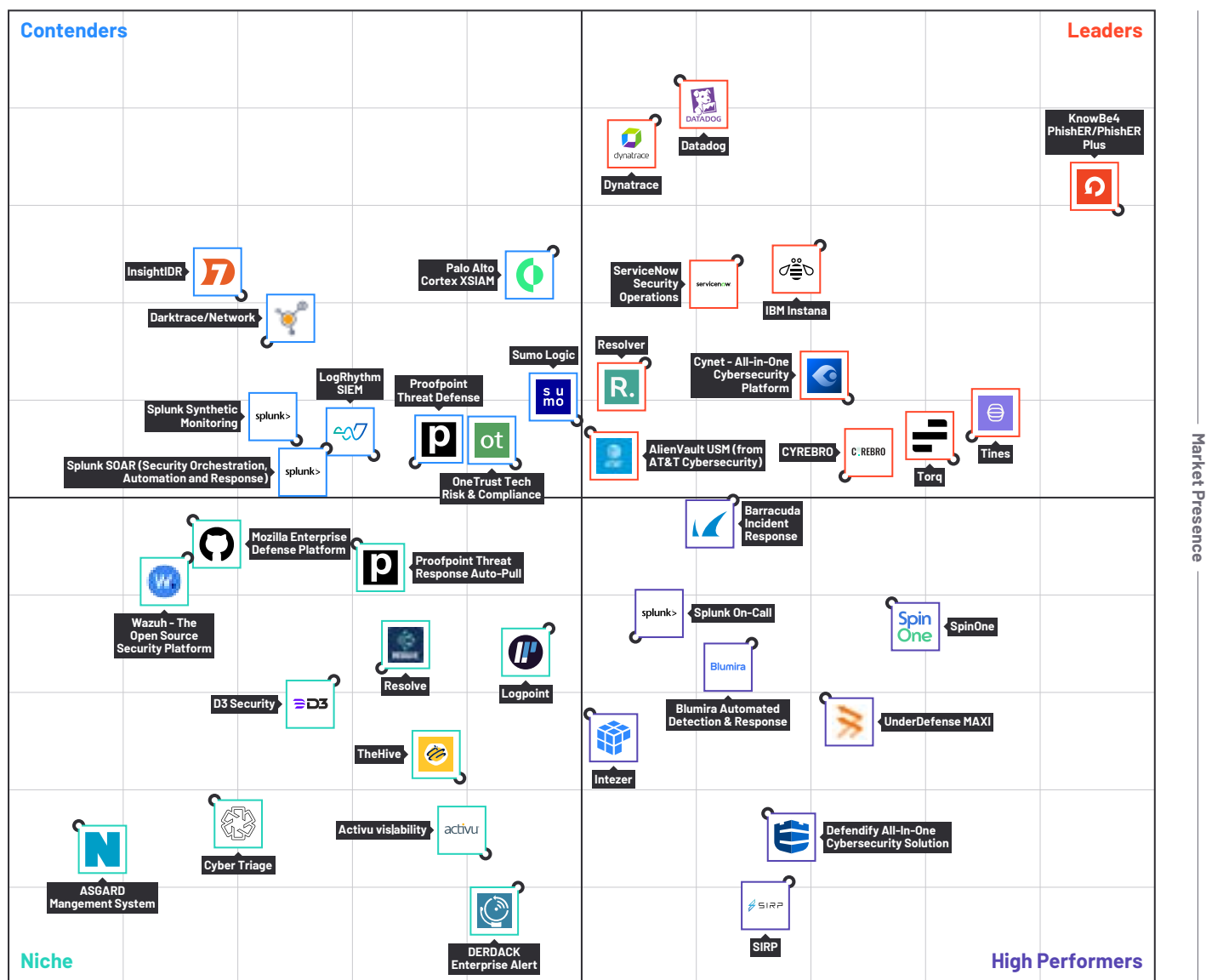


Grid® Report for Incident Response

Fall 2025



Incident Response Software



G2 Grid® Scoring

Satisfaction

(Incident Response Software continues on next page)

Incident Response Software (continued)

Incident Response Software Definition

Incident response software automates the process of and/or provides users with the tools necessary to find and resolve security breaches. Companies utilize the tools to monitor networks, infrastructure, and endpoints for intrusions and abnormal activity. They then use the programs to inspect and resolve intrusions and malware in the system. These products provide capabilities to resolve issues that arise after threats have bypassed firewalls and other security mechanisms. They alert administrators of unapproved access of applications and networks. They also have the ability to detect a variety of malware variants. Many tools automate the process of remedying these issues, but others guide users through known resolution processes.

Many incident response solutions function similarly to [security information and event management \(SIEM\)](#) software, but SIEM products provide a larger scope of security and IT management features.

To qualify for inclusion in the Incident Response category, a product must:

- ▶ Monitor for anomalies within an IT system
- ▶ Alert users of abnormal activity and detected malware
- ▶ Automate or guide users through remediation process
- ▶ Store incident data for analytics and reporting

Incident Response Grid® Scoring Description

Products shown on the Grid® for Incident Response have received a minimum of 10 reviews/ratings in data gathered by August 12, 2025. 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](#), [Datadog](#), [IBM Instana](#), [Dynatrace](#), [Tines](#), [ServiceNow Security Operations](#), [Torq](#), [Cynet - All-in-One Cybersecurity Platform](#), [CYREBRO](#), [Resolver](#), and [AlienVault USM](#) (from AT&T Cybersecurity)
- ▶ High Performing products have high customer Satisfaction scores and low Market Presence compared to the rest of the category. High Performers include: [SpinOne](#), [Barracuda Incident Response](#), [UnderDefense MAXI](#), [Blumira Automated Detection & Response](#), [Splunk On-Call](#), [Defendify All-In-One Cybersecurity Solution](#), [Intezer](#), and [SIRP](#)
- ▶ 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 Cortex XSIAM](#), [Sumo Logic](#), [OneTrust Tech Risk & Compliance](#), [InsightIDR](#), [Proofpoint Threat Response](#), [Darktrace/Network](#), [LogRhythm SIEM](#), [Splunk SOAR \(Security Orchestration, Automation and Response\)](#), and [Splunk Synthetic Monitoring](#)
- ▶ 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: [Logpoint](#), [Proofpoint Threat Response Auto-Pull](#), [Resolve](#), [Mozilla Enterprise Defense Platform](#), [TheHive](#), [Wazuh - The Open Source Security Platform](#), [D3 Security](#), [Activu visibility](#), [DERDACK Enterprise Alert](#), [Cyber Triage](#), and [ASGARD Mangement System](#)



Grid® Scores for Incident Response 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	418	100	83	91
Datadog	118	59	97	78
IBM Instana	28	72	79	75
Dynatrace	252	57	93	75
Tines	87	86	57	72
ServiceNow Security Operations	21	65	77	71
Torq	49	85	54	69
Cynet - All-in-One Cybersecurity Platform	121	75	61	68
CYREBRO	98	75	52	63
Resolver	75	56	65	61
AlienVault USM (from AT&T Cybersecurity)	28	51	57	54

High Performers

SpinOne	32	79	38	58
Barracuda Incident Response	13	64	49	57
UnderDefense MAXI	13	73	27	50
Blumira Automated Detection & Response	62	66	33	50
Splunk On-Call	15	55	34	44
Defendify All-in-One Cybersecurity Solution	28	67	14	41
Intezer	17	51	25	38
SIRP	22	69	6	38

(Grid® Scores for Incident Response 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 Incident Response 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 Cortex XSIAM	251	48	78	63
Sumo Logic	111	50	59	54
OneTrust Tech Risk & Compliance	28	44	54	49
InsightIDR	59	19	73	46
Proofpoint Threat Defense	16	35	54	44
Darktrace/Network	16	21	68	44
LogRhythm SIEM	95	31	55	43
Splunk SOAR (Security Orchestration, Automation and Response)	24	26	55	41
Splunk Synthetic Monitoring	12	24	56	40

(Grid® Scores for Incident Response 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 Incident Response 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.

Niche

	# of Reviews	Satisfaction	Market Presence	G2 Score
Logpoint	44	47	35	41
Proofpoint Threat Response Auto-Pull	24	29	45	37
Resolve	30	32	30	31
Mozilla Enterprise Defense Platform	10	14	47	31
TheHive	19	39	18	28
Wazuh - The Open Source Security Platform	40	14	43	28
D3 Security	63	27	29	28
Activu visibility	12	41	9	25
DERDACK Enterprise Alert	31	44	5	25
Cyber Triage	15	16	15	16
ASGARD Mangement System	13	4	12	8

* 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 Incident Response 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 Incident Response | Fall 2025 is based on reviews collected through August 12, 2025. We apply unique algorithms to this data to calculate Satisfaction (v4.0) and Market Presence (v7.0) scores for the Fall 2025 report quarter. To view the Incident Response Grid® with the most recent data, please visit the [Incident Response](#) 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 August 12, 2025. 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 software is not yet listed on G2 and it fits the market definition above, then users are encouraged to [suggest its addition](#) to our [Incident Response category](#).

Product Profiles

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

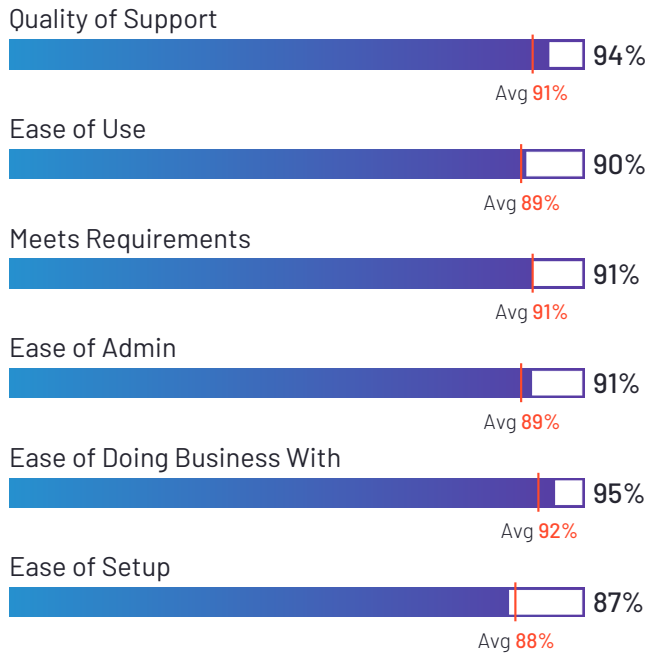


4.6 ★★★★★ (529)

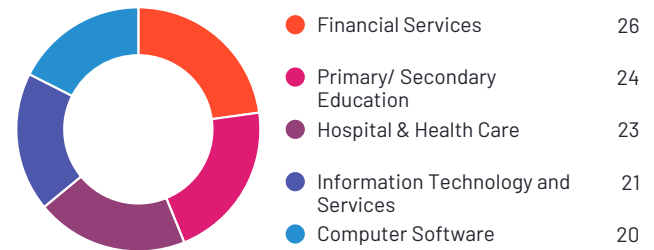


KnowBe4 PhishER/PhishER Plus has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. KnowBe4 PhishER/PhishER Plus received the highest Satisfaction score among products in Incident Response. 97% of users rated it 4 or 5 stars, 94% of users believe it is headed in the right direction, and users said they would be likely to recommend KnowBe4 PhishER/PhishER Plus at a rate of 91%. KnowBe4 PhishER/PhishER Plus is also in the Security Orchestration, Automation, and Response (SOAR) category.

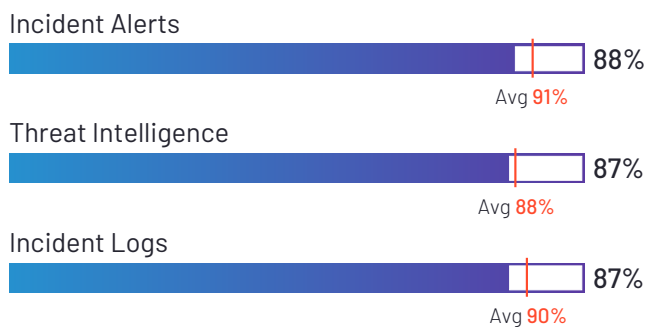
Satisfaction Ratings



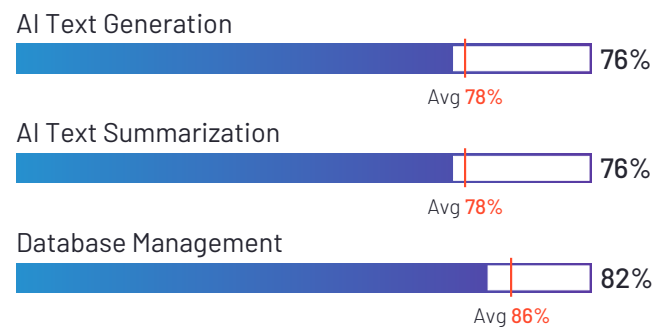
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
KnowBe4, Inc.



HQ Location
Clearwater, FL



Year Founded
2010



Employees (Listed On LinkedIn)
2,177



Company Website
knowbe4.com



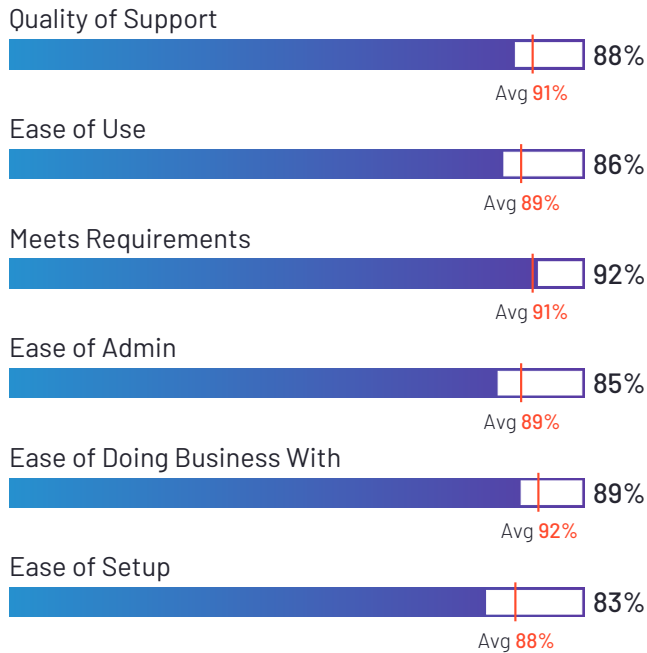
Datadog

4.4 ★★★★★ (640)

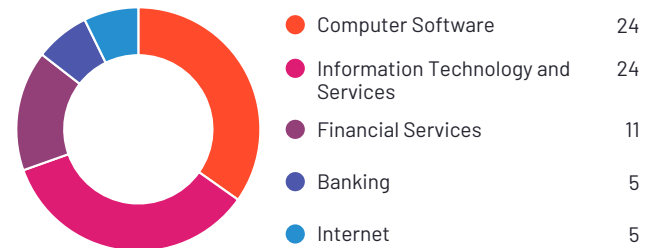


Datadog has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. Datadog has the largest Market Presence among products in Incident Response. 97% of users rated it 4 or 5 stars, 95% of users believe it is headed in the right direction, and users said they would be likely to recommend Datadog at a rate of 89%. Datadog is also in the Observability Pipeline, Observability Software, Enterprise Monitoring, Server Monitoring, Log Monitoring, AIOps Platforms, Network Traffic Analysis (NTA), Database Monitoring, IoT Device Management Platforms, IoT Analytics Platforms, Website Monitoring, Cloud Infrastructure Monitoring, IT Alerting, Container Monitoring, Log Analysis, Security Information and Event Management (SIEM), API Marketplace, Application Performance Monitoring (APM), Network Monitoring, and Cloud Cost Management categories.

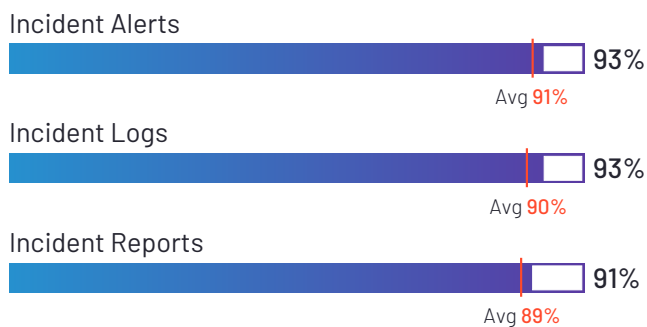
Satisfaction Ratings



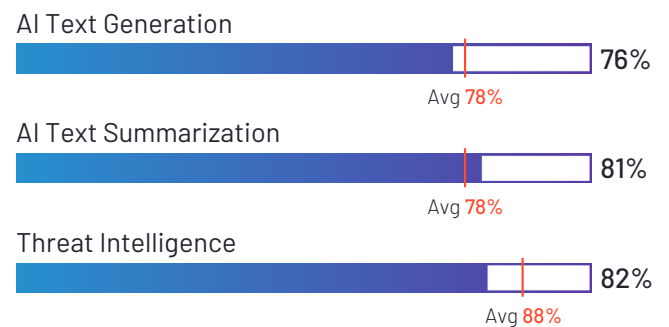
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Datadog



HQ Location
New York



Year Founded
2010



Employees (Listed On LinkedIn)
9,496



Company Website
datadoghq.com



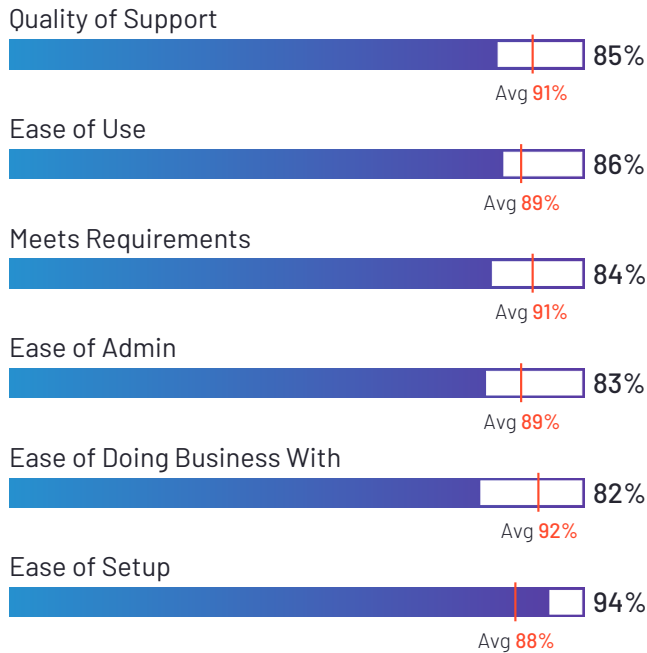
IBM Instana

4.4 ★★★★★ (399)

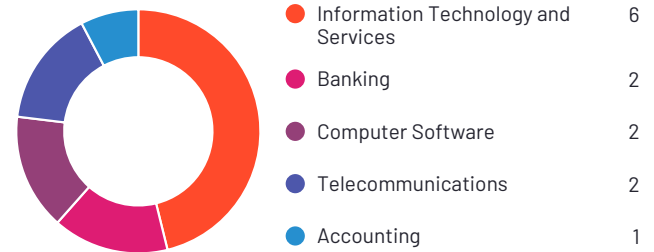


IBM Instana has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 86% of users rated it 4 or 5 stars, 84% of users believe it is headed in the right direction, and users said they would be likely to recommend IBM Instana at a rate of 82%. IBM Instana is also in the Observability Software, Enterprise Monitoring, Hardware Monitoring, AIOps Platforms, Database Monitoring, Website Monitoring, Cloud Infrastructure Monitoring, IT Alerting, Container Monitoring, Application Performance Monitoring (APM), Log Monitoring, Digital Experience Monitoring (DEM), and Server Monitoring 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)**
328,966



Company Website
www.ibm.com



dynatrace

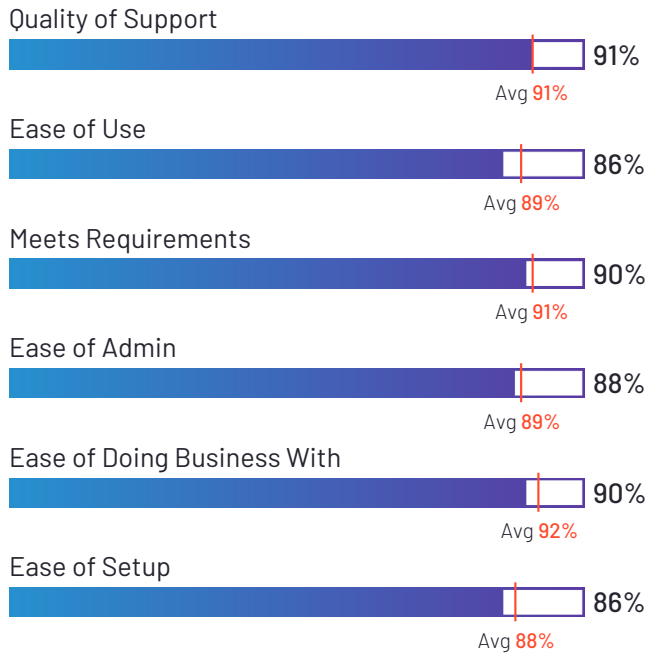
Dynatrace

4.5 ★★★★★ (1,337)

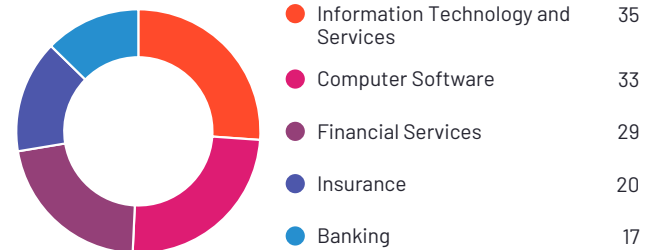


Dynatrace has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 97% of users rated it 4 or 5 stars, 92% of users believe it is headed in the right direction, and users said they would be likely to recommend Dynatrace at a rate of 92%. Dynatrace is also in the Observability Software, SAP Store, Enterprise Monitoring, Log Monitoring, AIOps Platforms, Database Monitoring, Digital Experience Monitoring (DEM), Website Monitoring, Cloud Infrastructure Monitoring, Runtime Application Self-Protection (RASP) Tools, ServiceNow Store Apps, Session Replay, IT Alerting, Container Monitoring, Log Analysis, Application Performance Monitoring (APM), Network Monitoring, and Bug Tracking categories.

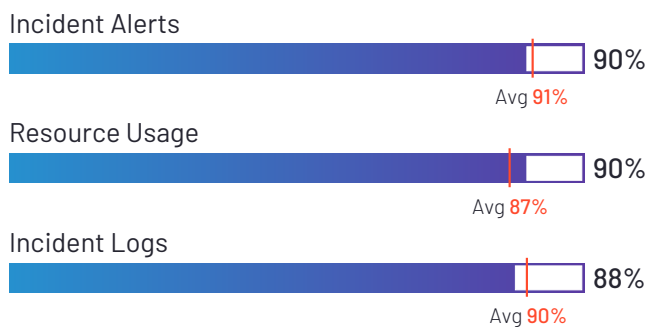
Satisfaction Ratings



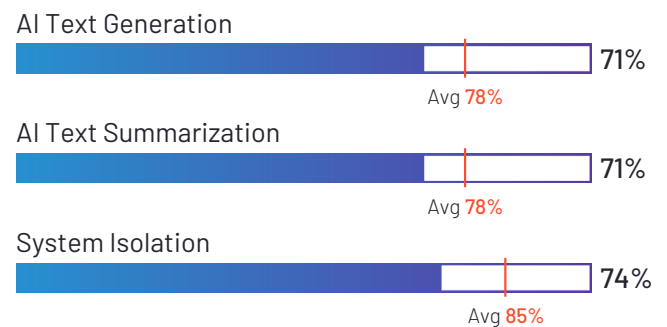
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Dynatrace



HQ Location
Waltham, MA



Year Founded
2005



Employees (Listed On LinkedIn)
5,533



Company Website
dynatrace.com



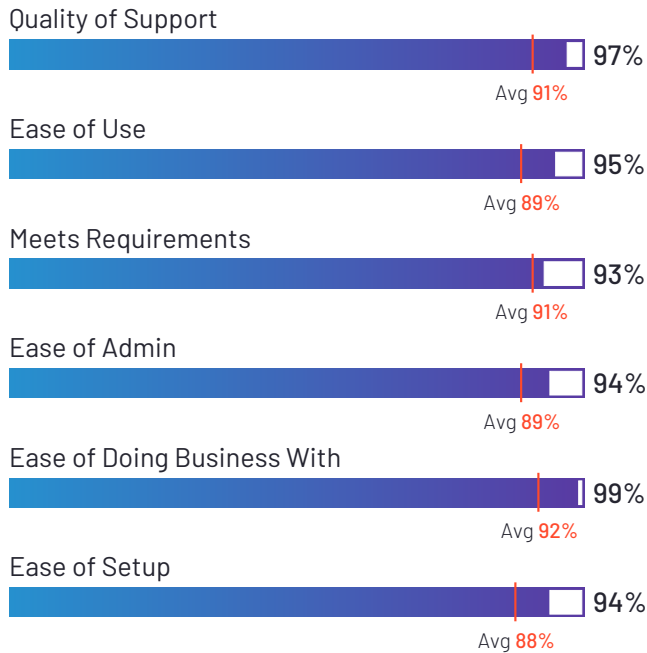
Tines

4.8 ★★★★★ (256)

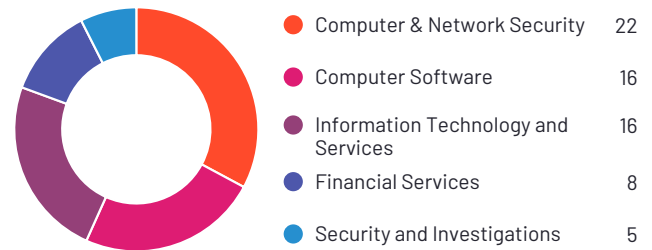


Tines has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 100% of users rated it 4 or 5 stars, 96% of users believe it is headed in the right direction, and users said they would be likely to recommend Tines at a rate of 96%. Tines is also in the Security Orchestration, Automation, and Response (SOAR), Workload Automation, iPaaS, Enterprise IT Management, and Other Process Automation categories.

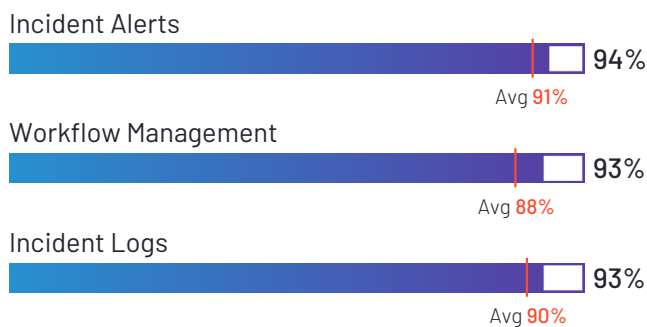
Satisfaction Ratings



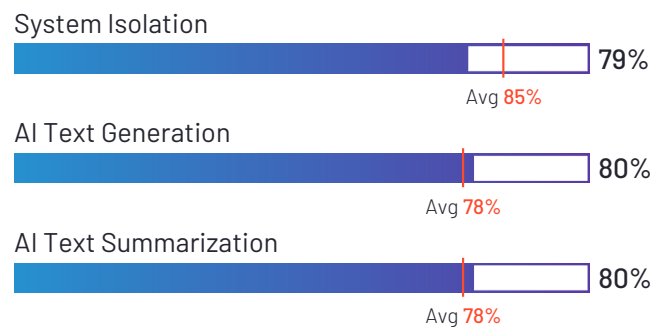
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Tines



HQ Location
Dublin, IE



Year Founded
2018



Employees (Listed On LinkedIn)
456



Company Website
www.tines.com

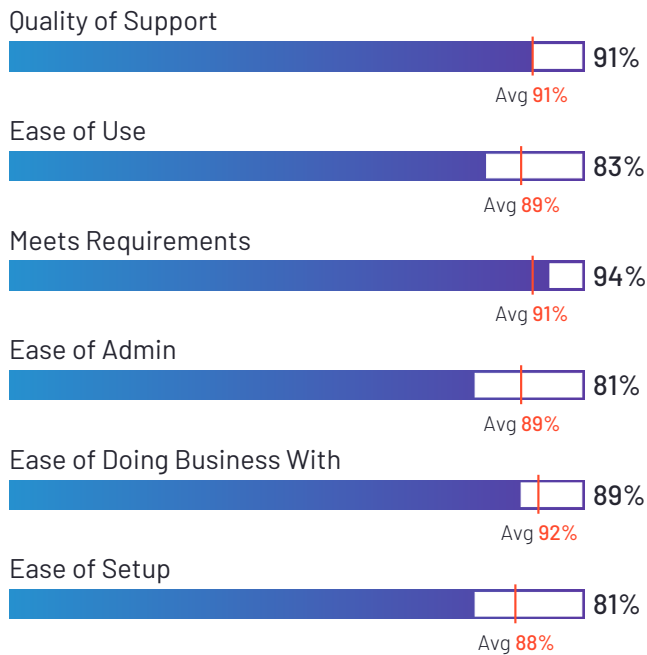
servicenow.

4.5 ★★★★★ (31)

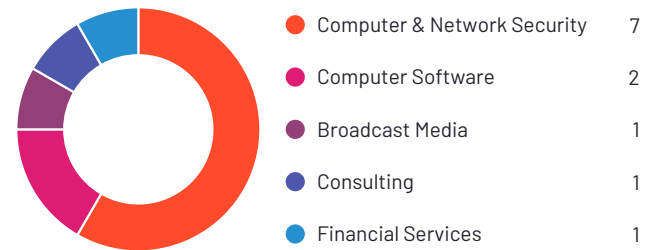


ServiceNow Security Operations has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 100% of users rated it 4 or 5 stars, 90% of users believe it is headed in the right direction, and users said they would be likely to recommend ServiceNow Security Operations at a rate of 88%. ServiceNow Security Operations is also in the Risk-Based Vulnerability Management, Security Orchestration, Automation, and Response (SOAR), and Threat Intelligence categories.

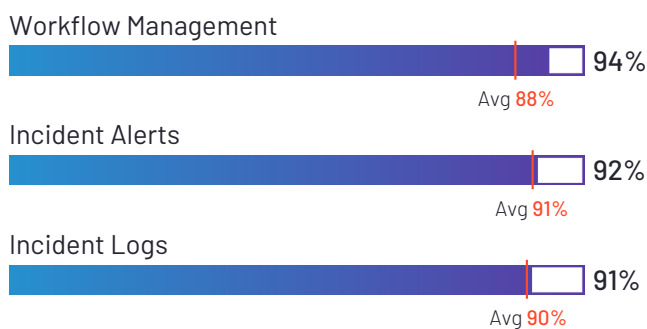
Satisfaction Ratings



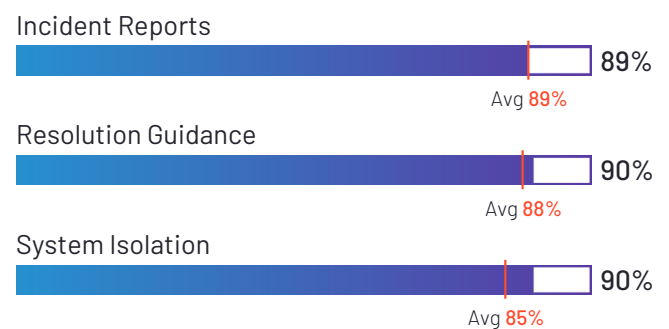
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
ServiceNow



HQ Location
Santa Clara, CA



Year Founded
2004



Employees (Listed On LinkedIn)
32,224



Company Website
servicenow.com



Torq

4.7 ★★★★★ (102)



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 96%. Torq is also in the Security Orchestration, Automation, and Response (SOAR), Identity and Access Management (IAM), Cloud Security Posture Management (CSPM), and AI SOC Agents categories.

Satisfaction Ratings

Quality of Support



Ease of Use



Meets Requirements



Ease of Admin



Ease of Doing Business With



Ease of Setup



Top Industries Represented



Highest-Rated Features

Workflow Management



Incident Alerts



Resolution Automation



Lowest-Rated Features

Database Management



Incident Logs



Incident Reports



Ownership
torq



HQ Location
New York, US



Year Founded
2020



Employees (Listed
On LinkedIn)
318



Company Website
torq.io



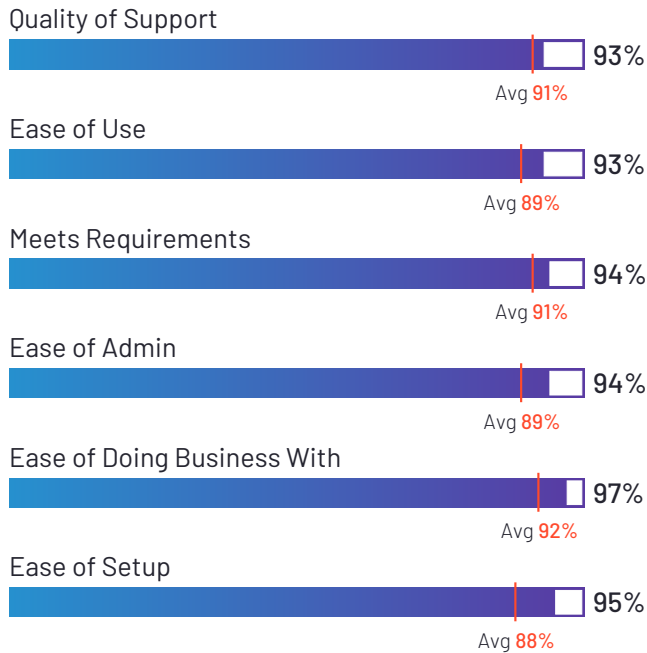
Cynet - All-in-One Cybersecurity Platform

4.7 ★★★★★ (217)

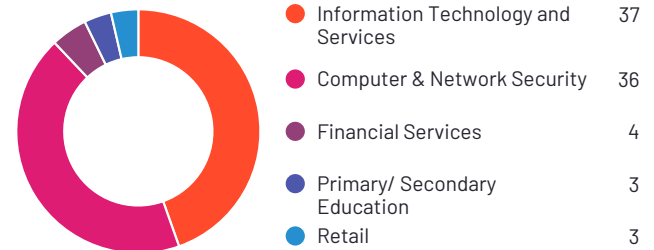


Cynet - All-in-One Cybersecurity Platform has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 99% of users rated it 4 or 5 stars, 96% of users believe it is headed in the right direction, and users said they would be likely to recommend Cynet - All-in-One Cybersecurity Platform at a rate of 95%. Cynet - All-in-One Cybersecurity Platform is also in the Extended Detection and Response (XDR) Platforms, Deception Technology, User and Entity Behavior Analytics (UEBA), Managed Detection and Response (MDR), Endpoint Protection Platforms, Endpoint Management, Endpoint Detection & Response (EDR), Security Information and Event Management (SIEM), and SaaS Security Posture Management (SSPM) Solutions categories.

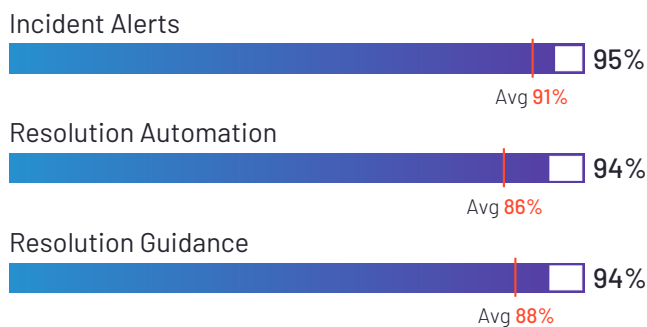
Satisfaction Ratings



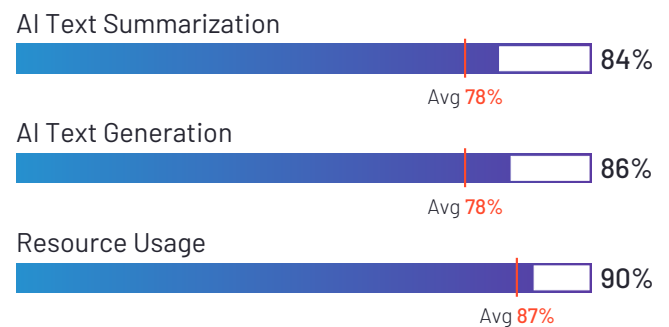
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Cynet



HQ Location
Boston, MA



Year Founded
2014



Employees (Listed On LinkedIn)
287



Company Website
www.cynet.com



CYREBRO

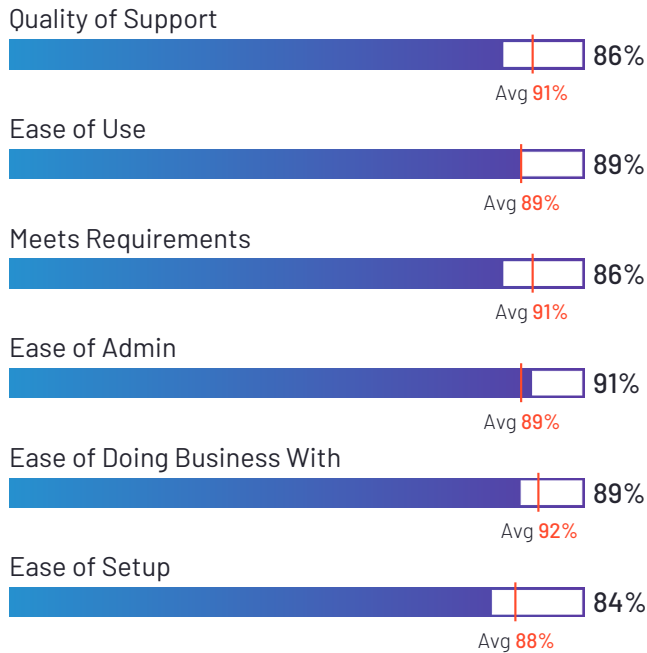
CYREBRO

4.3 ★★★★★ (129)

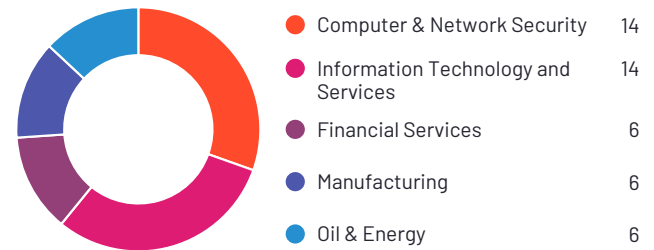


CYREBRO has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 90% of users rated it 4 or 5 stars, 90% of users believe it is headed in the right direction, and users said they would be likely to recommend CYREBRO at a rate of 87%. CYREBRO is also in the Managed Detection and Response (MDR) and Threat Intelligence categories.

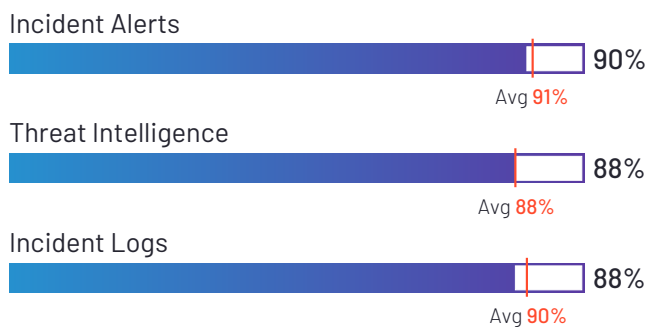
Satisfaction Ratings



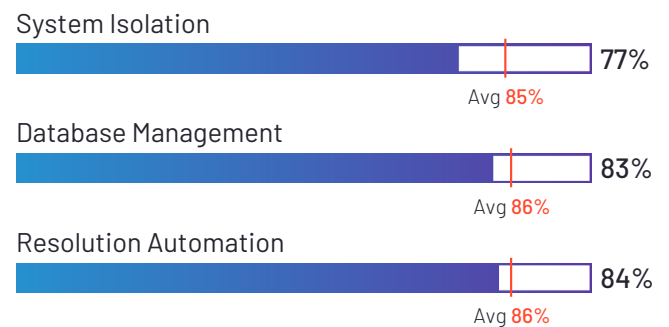
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
CYREBRO



HQ Location
Tel Aviv, IL



Year Founded
2013



Employees (Listed On LinkedIn)
100



Company Website
www.cyrebro.io



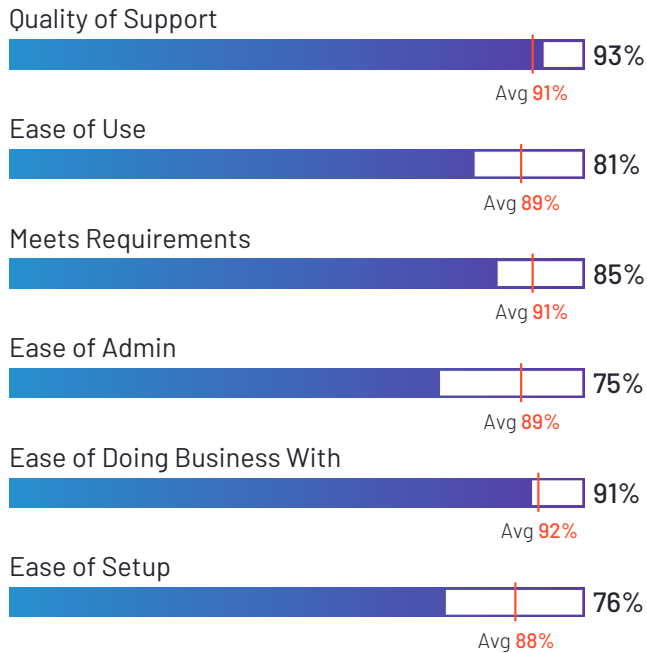
Resolver

4.3 ★★★★★ (169)



Resolver has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 96% of users rated it 4 or 5 stars, 87% of users believe it is headed in the right direction, and users said they would be likely to recommend Resolver at a rate of 88%. Resolver is also in the Content Moderation Tools, Security Compliance, Investigation Management, Enterprise Risk Management (ERM), Operational Risk Management, Third Party & Supplier Risk Management, IT Risk Management, Audit Management, Physical Security, and Threat Intelligence categories.

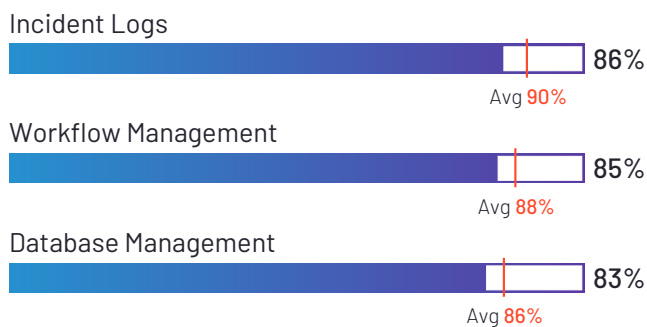
Satisfaction Ratings



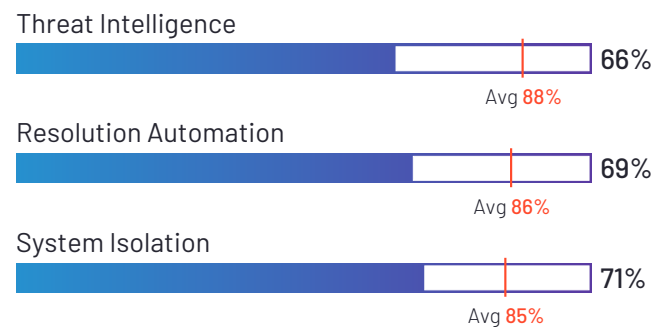
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Resolver



HQ Location
Toronto, Canada



**Employees (Listed
On LinkedIn)**
748



Company Website
resolver.com



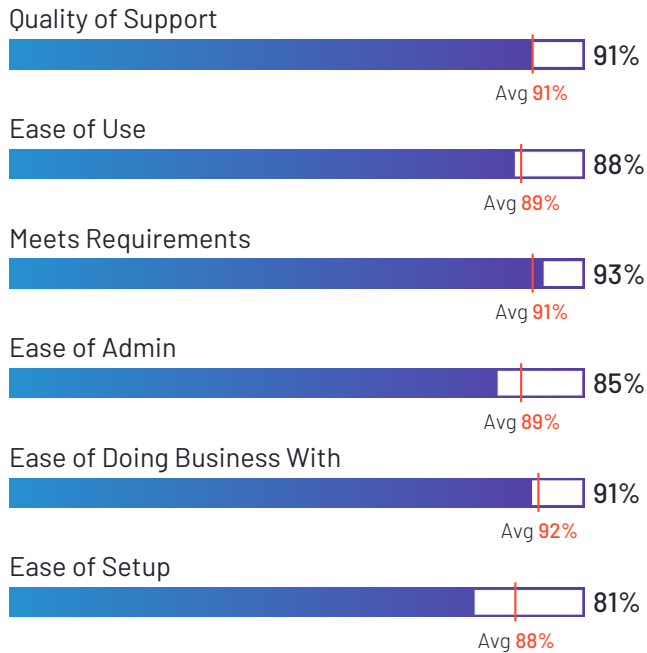
AlienVault USM (from AT&T Cybersecurity)

4.4 ★★★★★ (113)

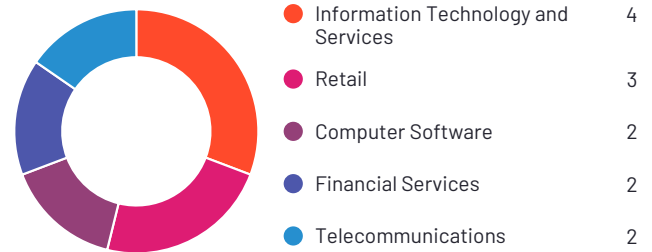


AlienVault USM (from AT&T Cybersecurity) has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 96% of users rated it 4 or 5 stars, 88% of users believe it is headed in the right direction, and users said they would be likely to recommend AlienVault USM (from AT&T Cybersecurity) at a rate of 91%. AlienVault USM (from AT&T Cybersecurity) is also in the Cloud Compliance, Intrusion Detection and Prevention Systems (IDPS), Vulnerability Scanner, and Security Information and Event Management (SIEM) categories.

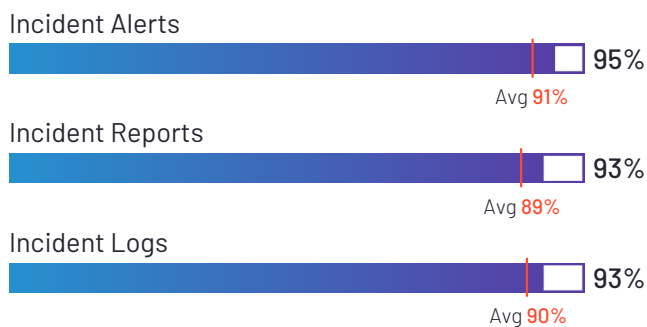
Satisfaction Ratings



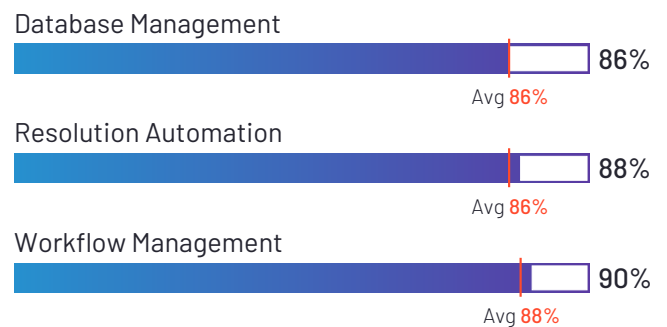
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
LevelBlue



HQ Location
Dallas, TX



Year Founded
1876



Employees (Listed On LinkedIn)
387



Company Website
levelblue.com



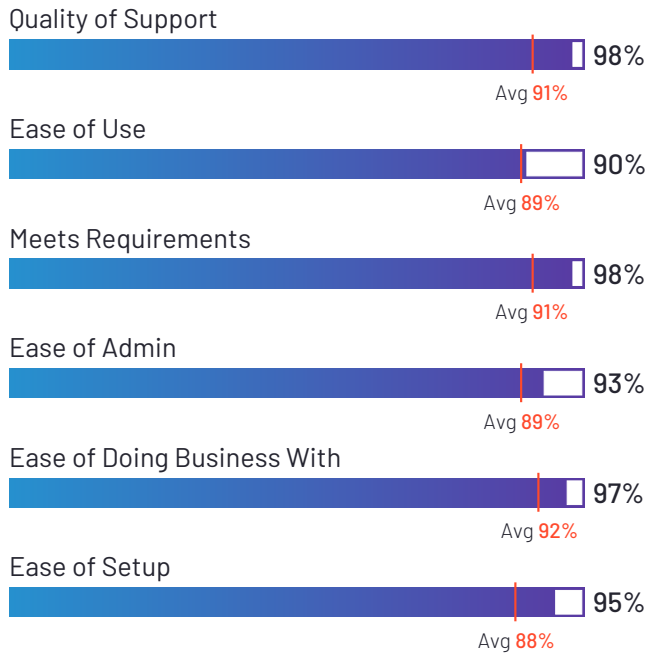
SpinOne

4.8 ★★★★★ (103)

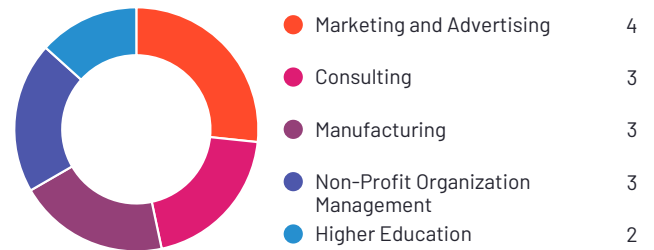


SpinOne has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend SpinOne at a rate of 97%. SpinOne is also in the SaaS Security Posture Management (SSPM) Solutions, Cloud File Security, Cloud Data Security, Data Loss Prevention (DLP), and SaaS Backup categories.

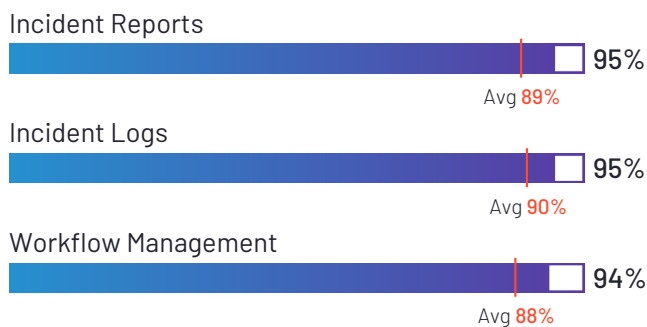
Satisfaction Ratings



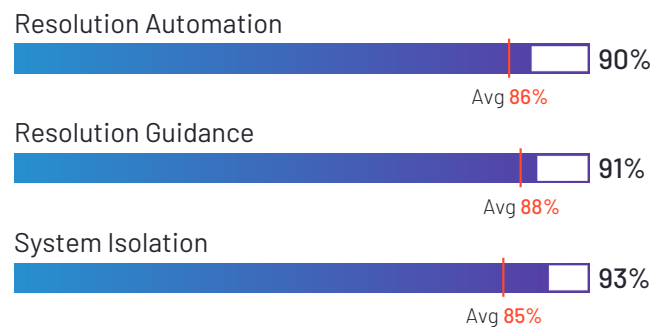
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
SpinAI



HQ Location
Palo Alto, California



Year Founded
2017



Employees (Listed On LinkedIn)
91



Company Website
spin.ai



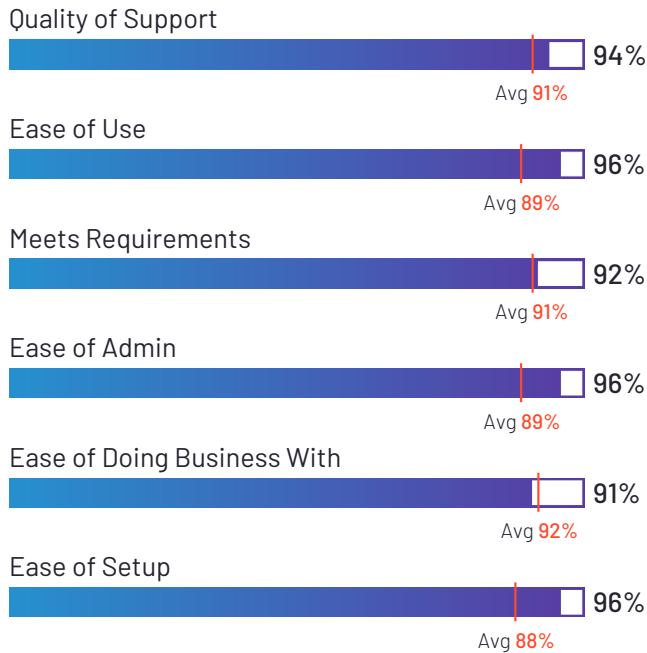
Barracuda Incident Response

4.5 ★★★★★ (14)

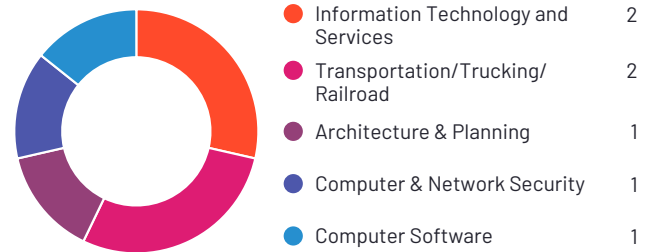


Barracuda Incident Response has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 92% of users rated it 4 or 5 stars, 91% of users believe it is headed in the right direction, and users said they would be likely to recommend Barracuda Incident Response at a rate of 90%. Barracuda Incident Response is also in the Security Orchestration, Automation, and Response (SOAR) category.

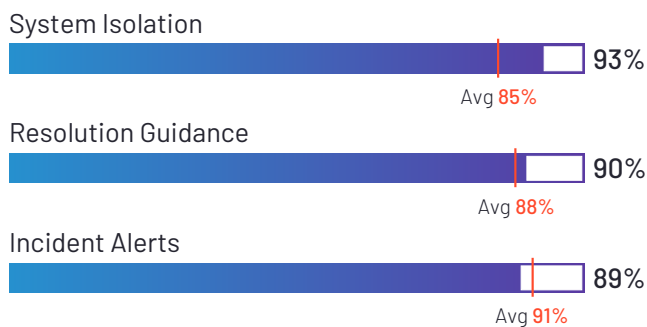
Satisfaction Ratings



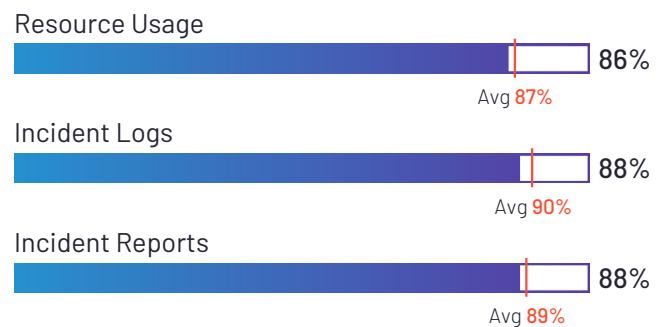
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Barracuda



HQ Location
Campbell, CA



Year Founded
2002



Employees (Listed On LinkedIn)
2,158



Company Website
barracuda.com



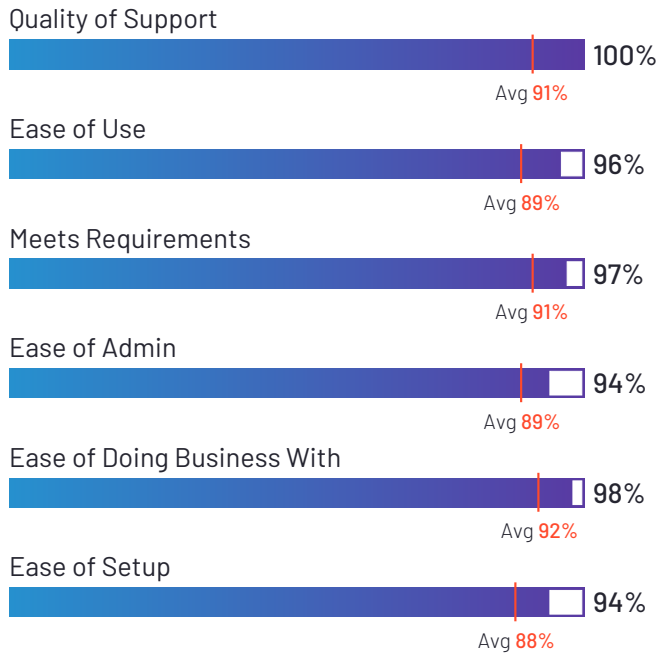
UnderDefense MAXI

4.8 ★★★★★ (26)

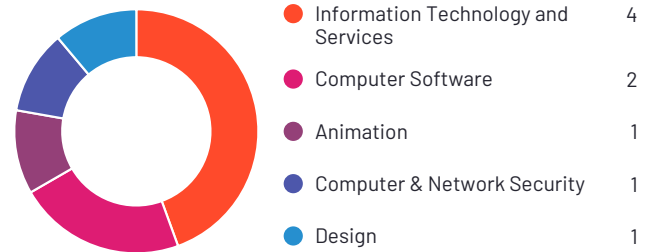


UnderDefense MAXI has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend UnderDefense MAXI at a rate of 95%. UnderDefense MAXI is also in the Managed Detection and Response (MDR) category.

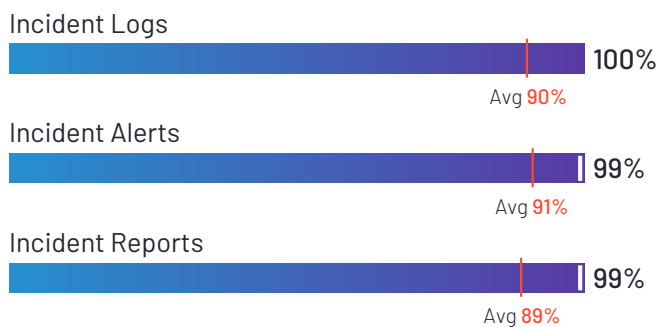
Satisfaction Ratings



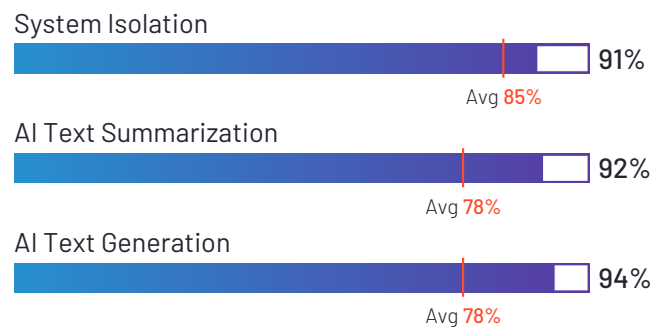
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
UnderDefense



HQ Location
New York, NY



Year Founded
2017



Employees (Listed On LinkedIn)
119



Company Website
underdefense.com

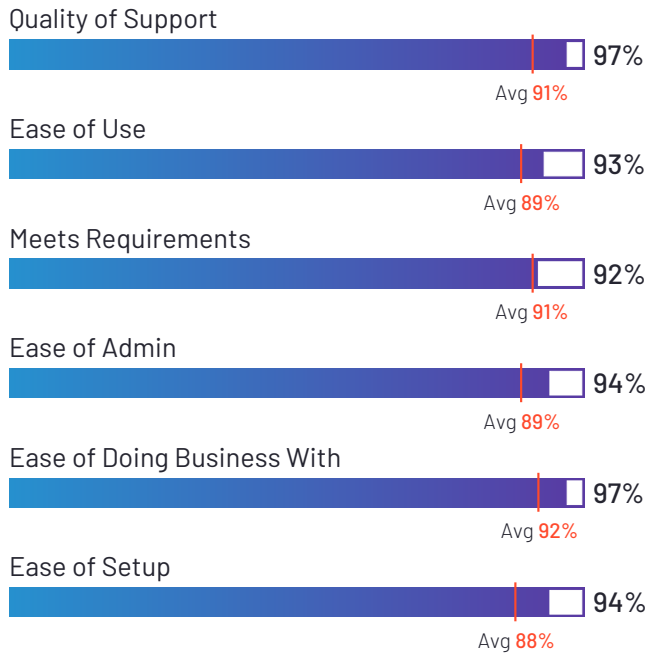
Blumira

4.6 ★★★★★ (119)

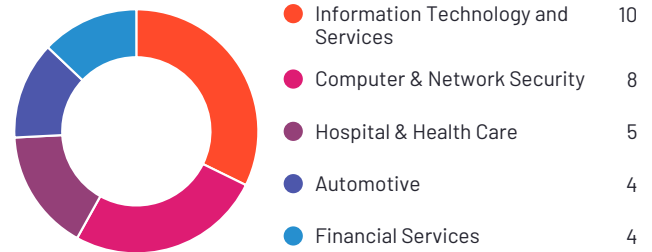


Blumira Automated Detection & Response has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Blumira Automated Detection & Response at a rate of 95%. Blumira Automated Detection & Response is also in the Network Detection and Response (NDR), Cloud Security Monitoring and Analytics, Security Orchestration, Automation, and Response (SOAR), Log Monitoring, Managed Detection and Response (MDR), Intrusion Detection and Prevention Systems (IDPS), Security Information and Event Management (SIEM), and Extended Detection and Response (XDR) Platforms categories.

Satisfaction Ratings



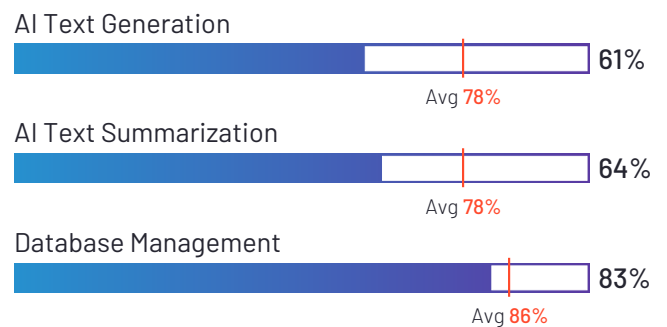
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Blumira



HQ Location
Ann Arbor, Michigan



Year Founded
2018



Employees (Listed
On LinkedIn)
65



Company Website
blumira.com

splunk>

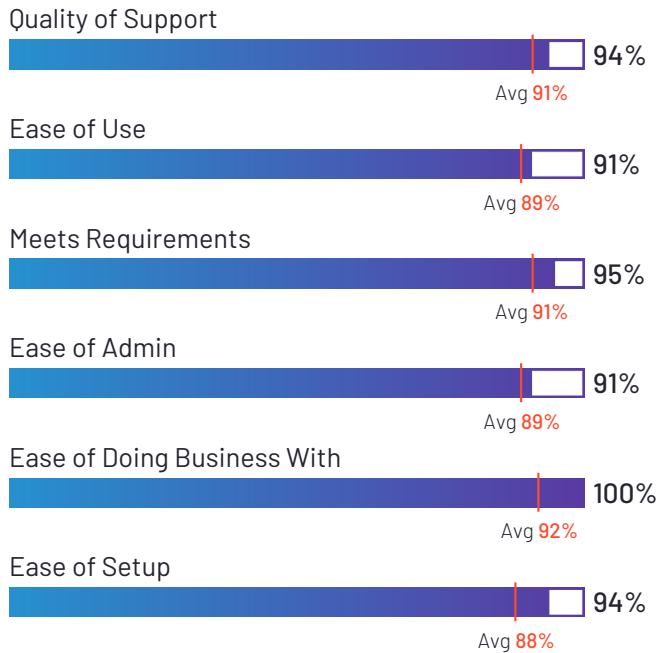
Splunk On-Call

4.6 ★★★★★ (50)

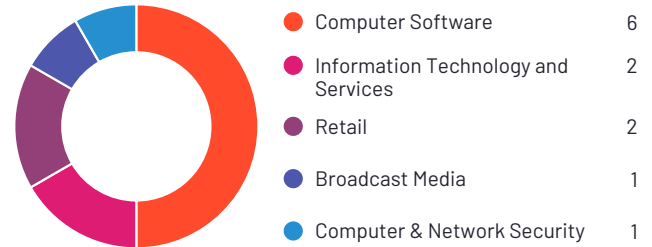


Splunk On-Call has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 93% of users believe it is headed in the right direction, and users said they would be likely to recommend Splunk On-Call at a rate of 95%. Splunk On-Call is also in the IT Alerting and Incident Management categories.

Satisfaction Ratings



Top Industries Represented



Ownership
Cisco



HQ Location
San Jose, CA



Year Founded
1984



Employees (Listed On LinkedIn)
94,810



Company Website
www.cisco.com

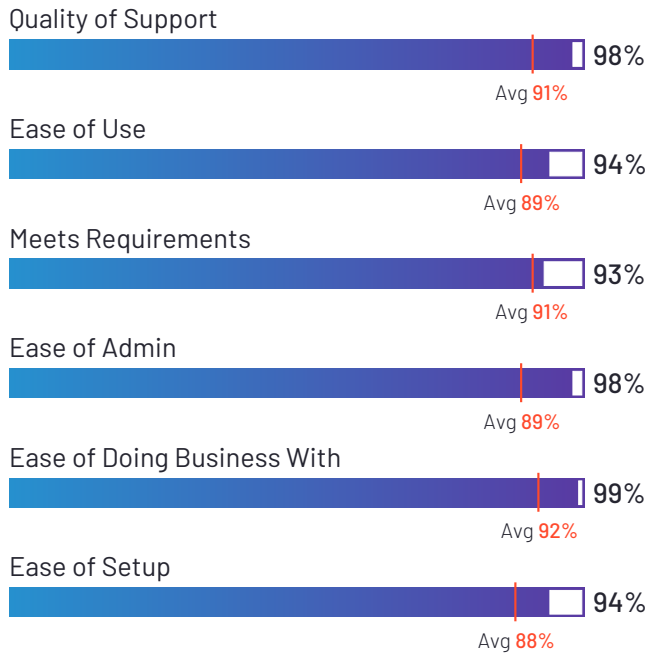
DEFENDIFY

4.7 ★★★★★ (57)

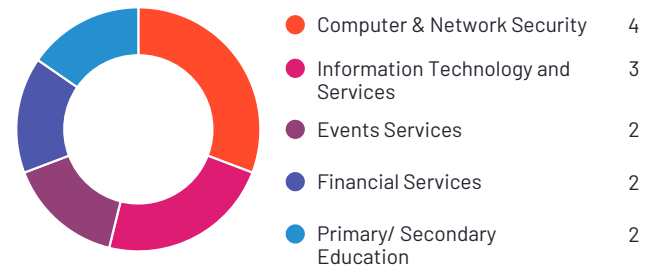


Defendify All-In-One Cybersecurity Solution has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 100% of users rated it 4 or 5 stars, 94% of users believe it is headed in the right direction, and users said they would be likely to recommend Defendify All-In-One Cybersecurity Solution at a rate of 96%. Defendify All-In-One Cybersecurity Solution is also in the Dark Web Monitoring, Breach and Attack Simulation (BAS), Managed Detection and Response (MDR), Penetration Testing, Website Security, Vulnerability Scanner, Security Awareness Training, Threat Intelligence, and Vulnerability Management categories.

Satisfaction Ratings



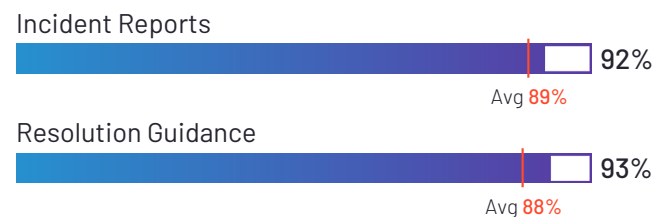
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Defendify



HQ Location
Portland, Maine



Year Founded
2017



Employees (Listed On LinkedIn)
36



Company Website
defendify.com



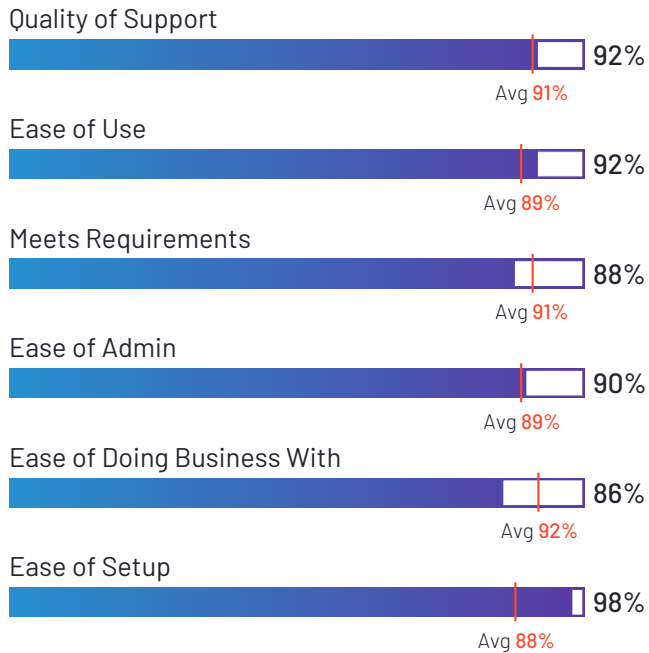
Intezer

4.5 ★★★★★ (192)

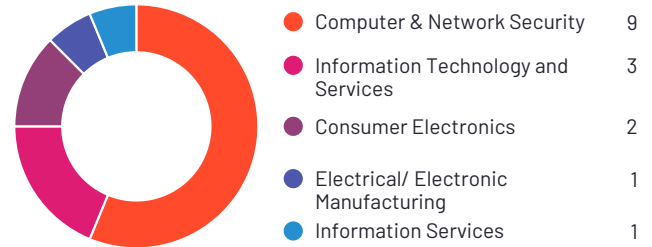


Intezer has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 94% of users rated it 4 or 5 stars, 92% of users believe it is headed in the right direction, and users said they would be likely to recommend Intezer at a rate of 89%. Intezer is also in the Malware Analysis Tools, Network Sandboxing, Threat Intelligence, Managed Detection and Response (MDR), Security Orchestration, Automation, and Response (SOAR), Endpoint Detection & Response (EDR), and AI SOC Agents categories.

Satisfaction Ratings



Top Industries Represented



Ownership
Intezer



HQ Location
New York



Year Founded
2015



Employees (Listed On LinkedIn)
60



Company Website
intezer.com



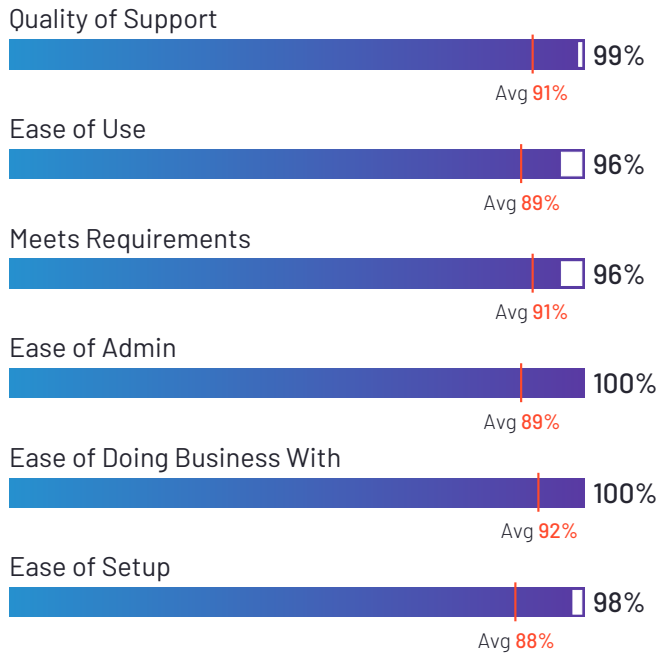
SIRP

4.7 ★★★★★ (27)

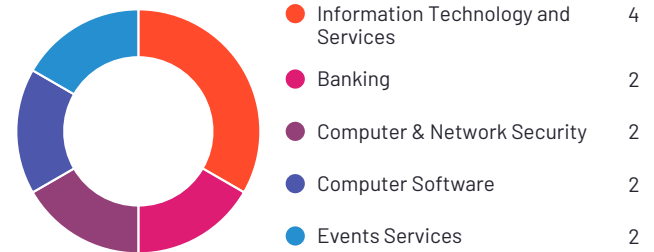


SIRP has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 95% of users rated it 4 or 5 stars, 90% of users believe it is headed in the right direction, and users said they would be likely to recommend SIRP at a rate of 94%. SIRP is also in the Threat Intelligence and Security Orchestration, Automation, and Response (SOAR) categories.

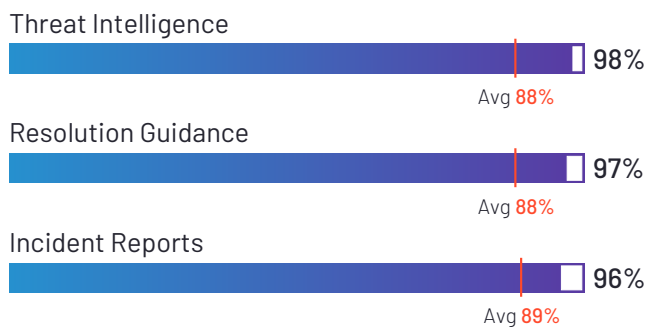
Satisfaction Ratings



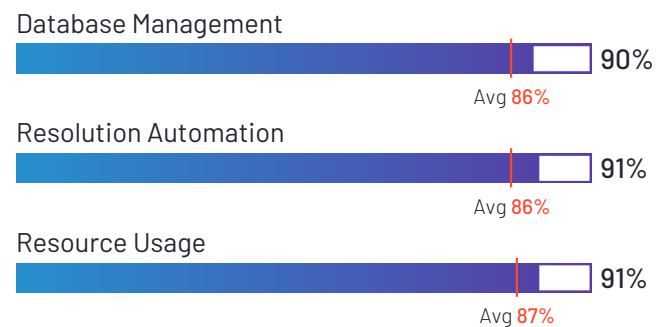
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
SIRP



HQ Location
London



Year Founded
2017



Employees (Listed
On LinkedIn)
52



Company Website
www.sirp.io

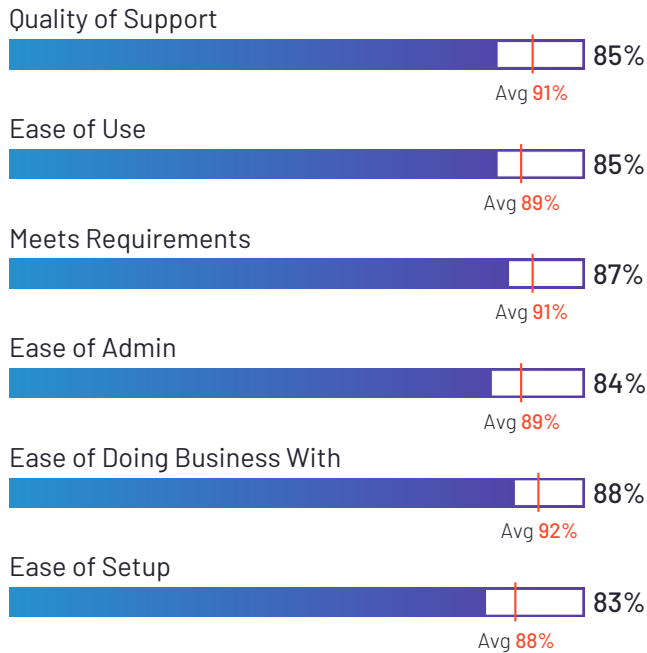


Palo Alto Cortex XSIAM

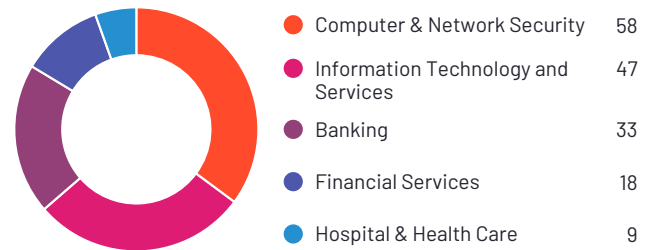
4.3 ★★★★★ (474)

Palo Alto Cortex XSIAM 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. 93% 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 Palo Alto Cortex XSIAM at a rate of 87%. Palo Alto Cortex XSIAM is also in the Security Information and Event Management (SIEM), Cloud Security Monitoring and Analytics, User and Entity Behavior Analytics (UEBA), Digital Forensics, Network Traffic Analysis (NTA), Extended Detection and Response (XDR) Platforms, Security Orchestration, Automation, and Response (SOAR), Data Breach Notification, Endpoint Detection & Response (EDR), and Risk-Based Vulnerability Management categories.

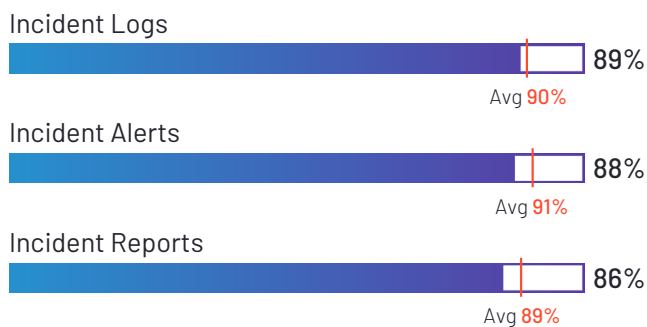
Satisfaction Ratings



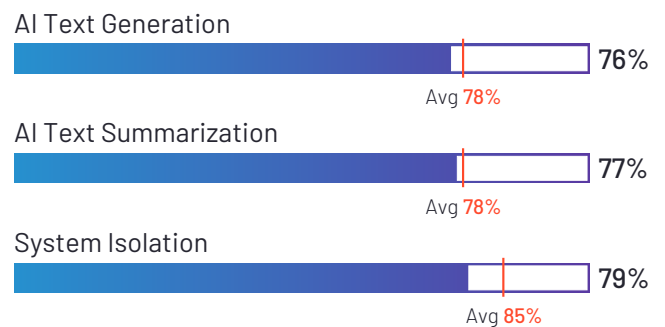
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Palo Alto Networks



HQ Location
Santa Clara, CA



Year Founded
2005



Employees (Listed On LinkedIn)
17,526



Company Website
paloaltonetworks.com



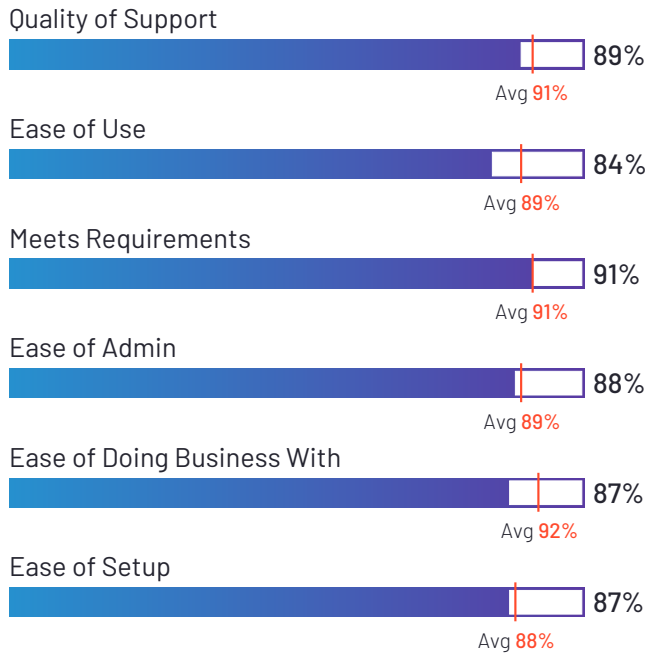
sumo logic

Sumo Logic

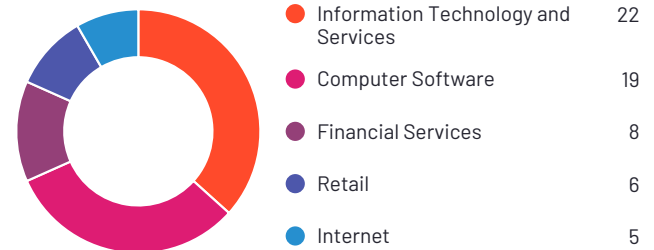
4.3 ★★★★★ (344)

Sumo Logic 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. 96% of users rated it 4 or 5 stars, 88% 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 88%. Sumo Logic is also in the Cloud Security Monitoring and Analytics, Log Monitoring, Cloud Infrastructure Monitoring, Container Monitoring, Log Analysis, Security Information and Event Management (SIEM), Application Performance Monitoring (APM), Security Orchestration, Automation, and Response (SOAR), and Observability Software categories.

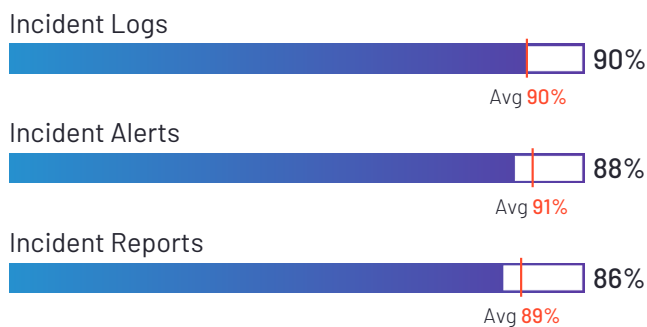
Satisfaction Ratings



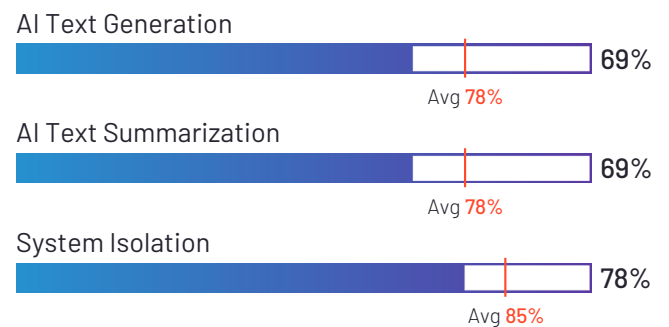
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Sumo Logic



HQ Location
Redwood City, CA



Year Founded
2010



Employees (Listed On LinkedIn)
901



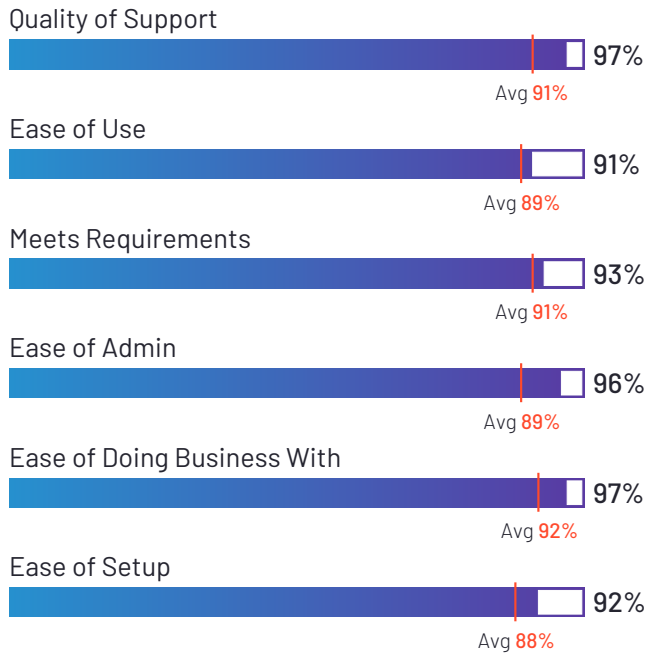
Company Website
sumologic.com

onetrust

4.5 ★★★★★ (102)

OneTrust Tech Risk & Compliance 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, 93% of users believe it is headed in the right direction, and users said they would be likely to recommend OneTrust Tech Risk & Compliance at a rate of 94%. OneTrust Tech Risk & Compliance is also in the Security Compliance, Vendor Security and Privacy Assessment, Enterprise Risk Management (ERM), Policy Management, and IT Risk Management categories.

Satisfaction Ratings



Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
OneTrust



HQ Location
Atlanta, Georgia



Year Founded
2016



**Employees (Listed
On LinkedIn)**
2,576



Company Website
onetrust.com

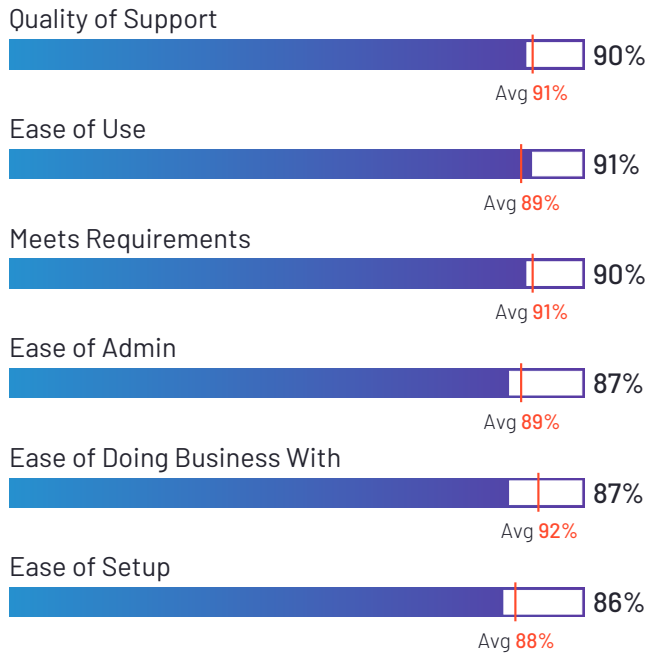


InsightIDR

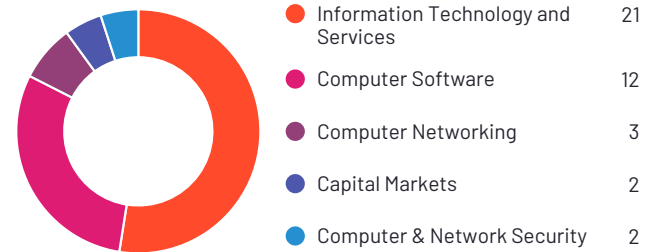
4.4 ★★★★★ (70)

InsightIDR 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, 89% of users believe it is headed in the right direction, and users said they would be likely to recommend InsightIDR at a rate of 88%. InsightIDR is also in the Network Detection and Response (NDR), User and Entity Behavior Analytics (UEBA), Network Traffic Analysis (NTA), Security Information and Event Management (SIEM), and Extended Detection and Response (XDR) Platforms categories.

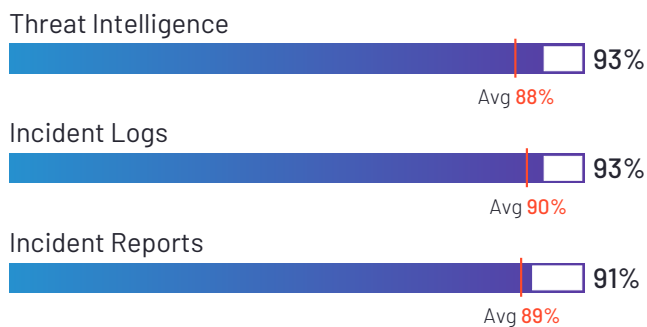
Satisfaction Ratings



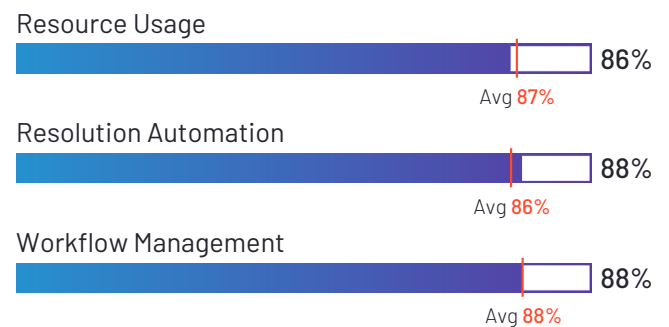
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Rapid7



HQ Location
Boston, MA



Year Founded
2000



Employees (Listed
On LinkedIn)
3,035



Company Website
www.rapid7.com

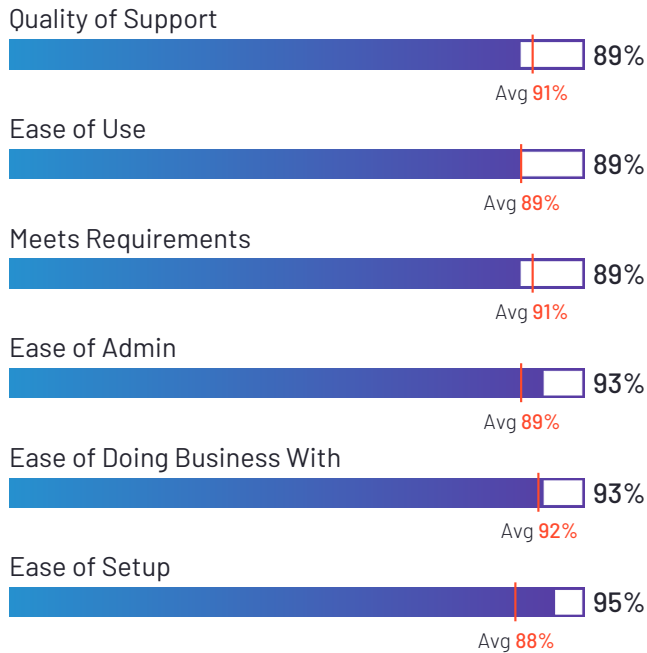


Proofpoint Threat Response

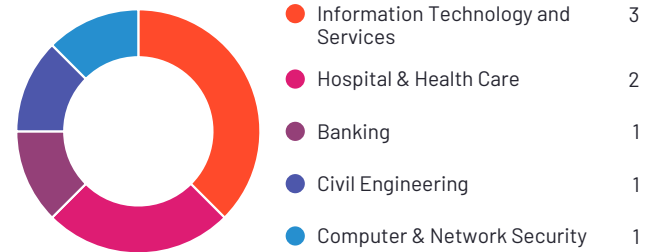
4.6 ★★★★★ (17)

Proofpoint Threat 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. 100% 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 Proofpoint Threat Defense at a rate of 91%. Proofpoint Threat Defense is also in the Security Orchestration, Automation, and Response (SOAR) category.

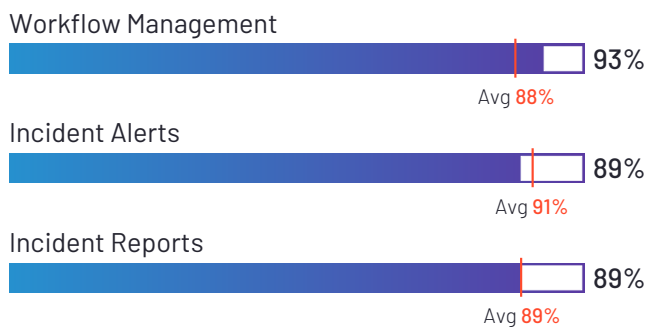
Satisfaction Ratings



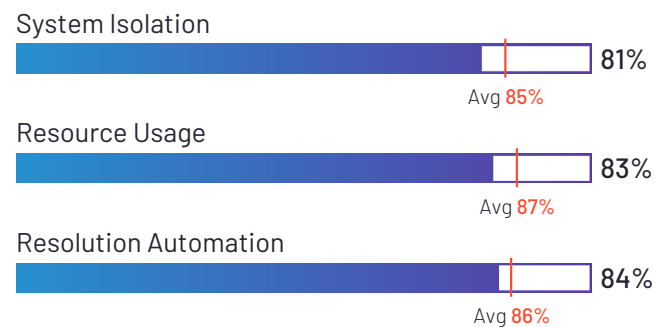
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Proofpoint



HQ Location
Sunnyvale, CA



Year Founded
2002



Employees (Listed On LinkedIn)
4,845



Company Website
proofpoint.com

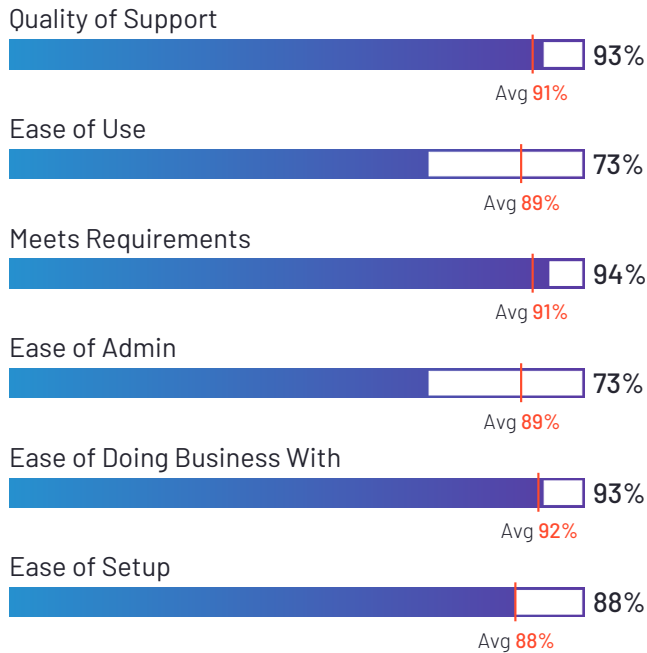


Darktrace/Network

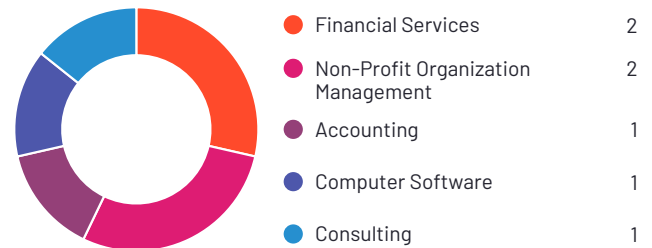
4.5 ★★★★★ (17)

Darktrace/Network 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, 91% of users believe it is headed in the right direction, and users said they would be likely to recommend Darktrace/Network at a rate of 89%. Darktrace/Network is also in the Network Traffic Analysis (NTA), Managed Detection and Response (MDR), Network Monitoring, Network Detection and Response (NDR), Cloud Detection and Response (CDR), Intrusion Detection and Prevention Systems (IDPS), Cloud Workload Protection Platforms, and Cloud Security Monitoring and Analytics categories.

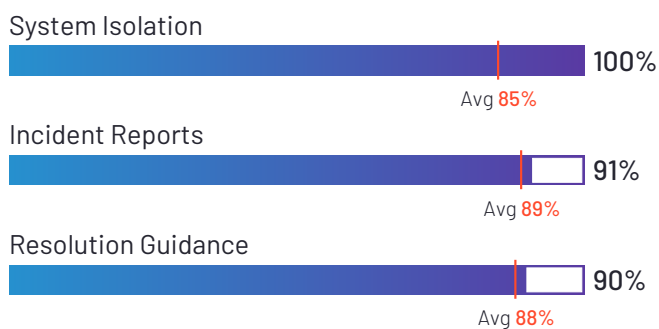
Satisfaction Ratings



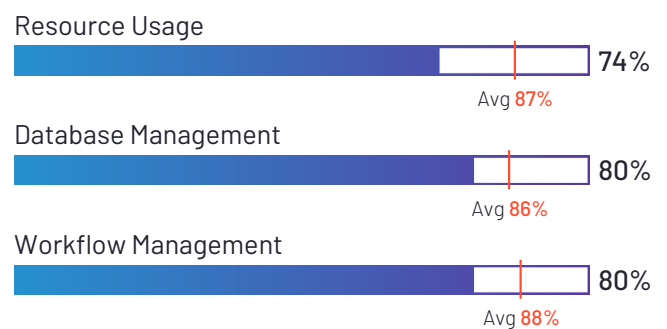
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Darktrace



HQ Location
Cambridgeshire,
England



Year Founded
2013



**Employees (Listed
On LinkedIn)**
2,575



Company Website
darktrace.com

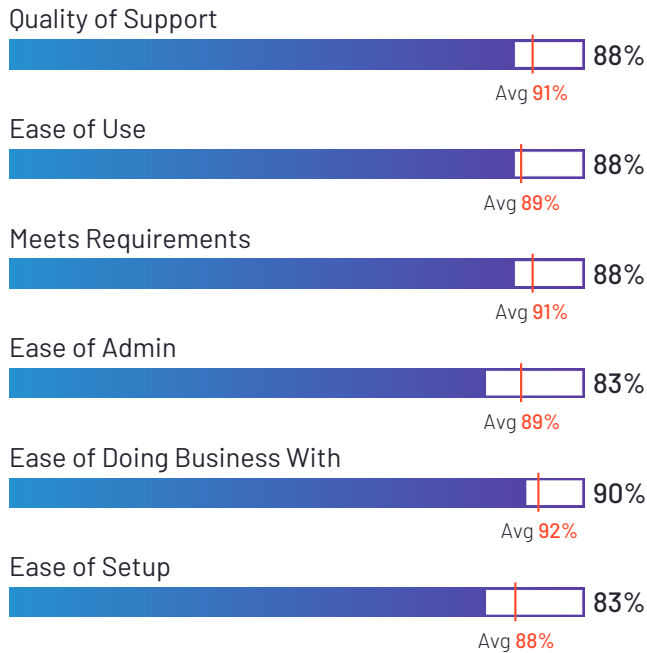


LogRhythm SIEM

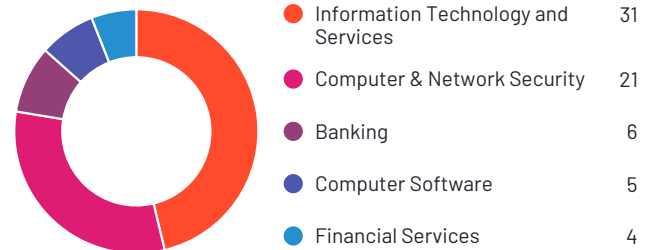
4.2 ★★★★★ (152)

LogRhythm SIEM 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. 98% 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 LogRhythm SIEM at a rate of 87%. LogRhythm SIEM is also in the Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) Platforms categories.

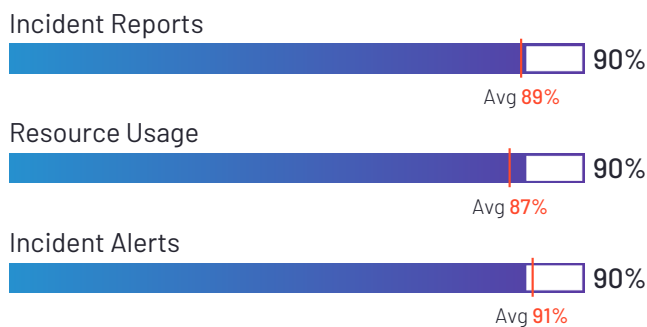
Satisfaction Ratings



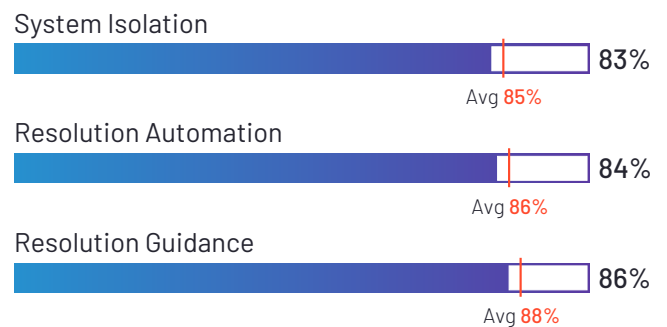
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Exabeam



HQ Location
Foster City, US



Year Founded
2013



Employees (Listed On LinkedIn)
907



Company Website
exabeam.com

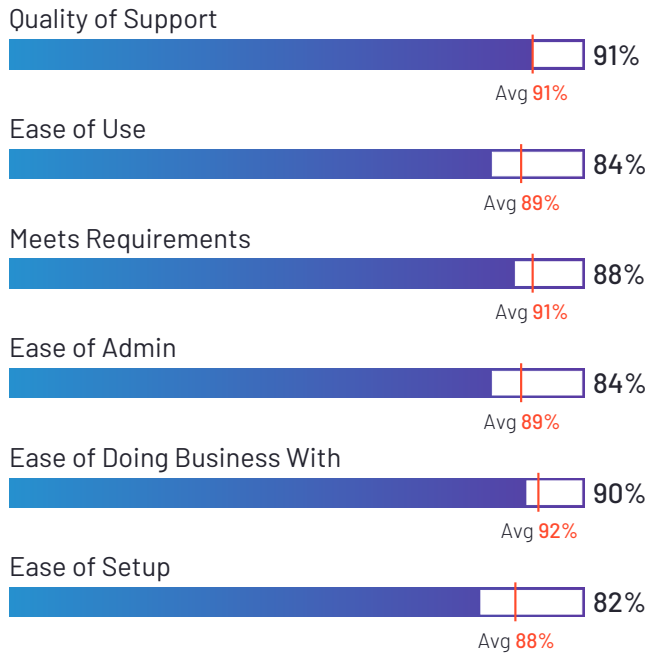
splunk>

Splunk SOAR (Security Orchestration, Automation and Response)

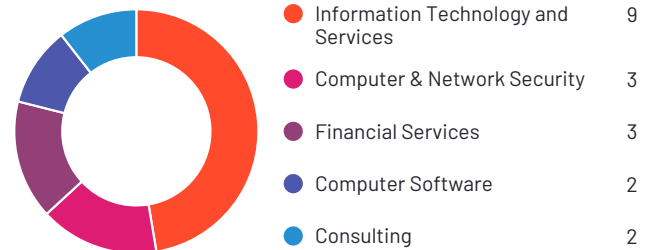
4.4 ★★★★★ (40)

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. 88% 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 Splunk SOAR (Security Orchestration, Automation and Response) at a rate of 88%. Splunk SOAR (Security Orchestration, Automation and Response) is also in the Security Orchestration, Automation, and Response (SOAR) category.

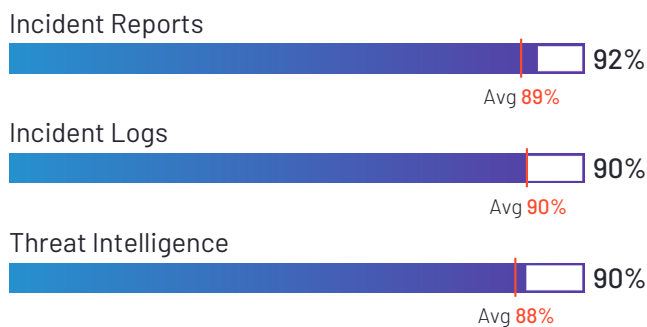
Satisfaction Ratings



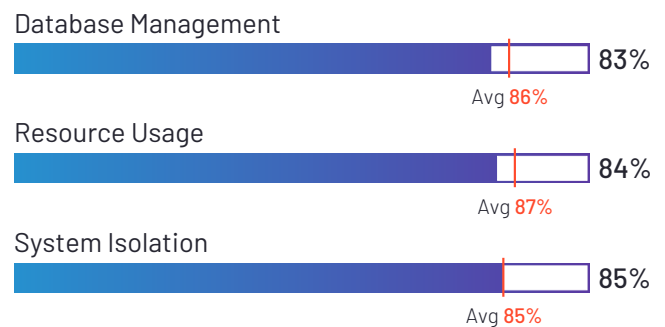
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Cisco



HQ Location
San Jose, CA



Year Founded
1984



Employees (Listed On LinkedIn)
94,810



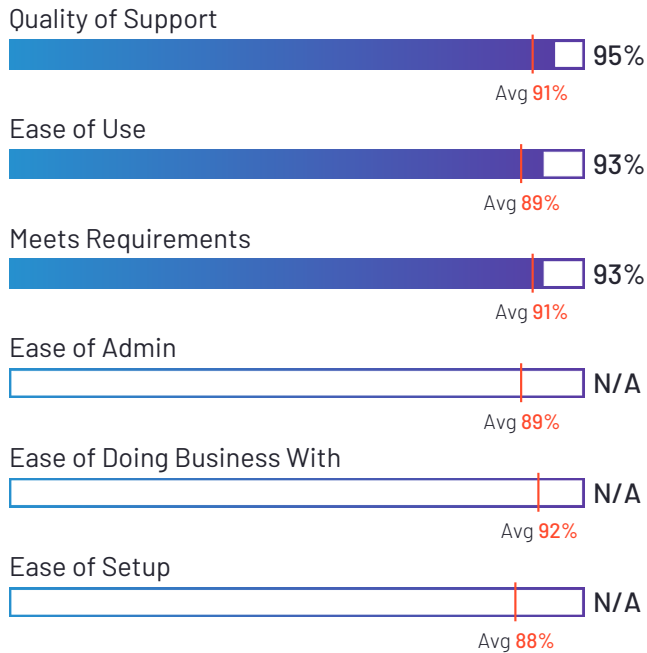
Company Website
www.cisco.com

splunk>

4.5 ★★★★★ (25)

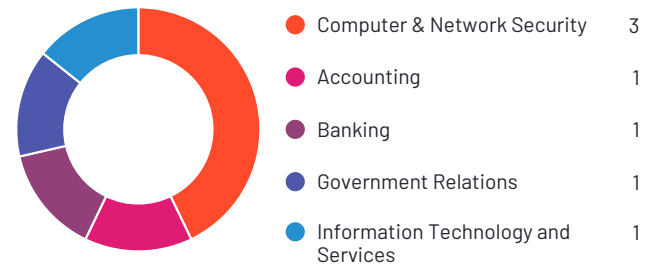
Splunk Synthetic Monitoring has been named a Contender product based on having a relatively low customer Satisfaction score and large Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Splunk Synthetic Monitoring at a rate of 90%. Splunk Synthetic Monitoring is also in the Digital Experience Monitoring (DEM), Application Performance Monitoring (APM), Cloud Security Monitoring and Analytics, and Digital Forensics categories.

Satisfaction Ratings

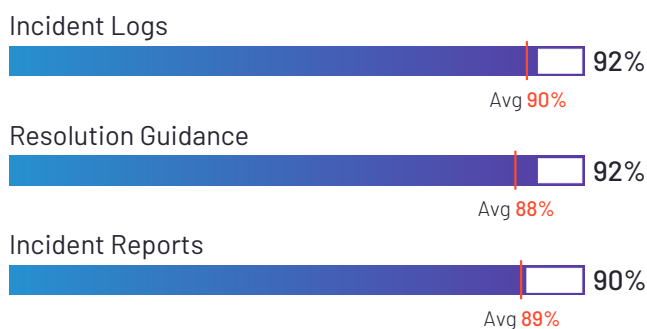


*N/A is displayed when fewer than five responses were received for the question.

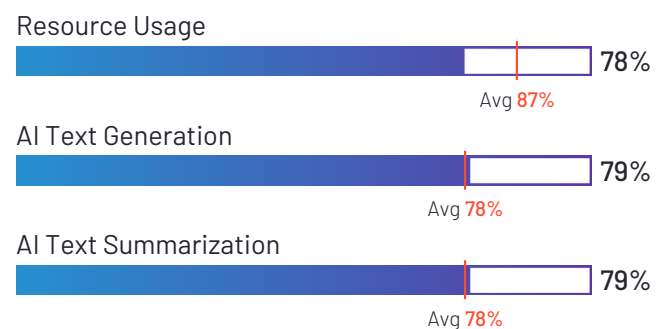
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Cisco



HQ Location
San Jose, CA



Year Founded
1984



Employees (Listed On LinkedIn)
94,810



Company Website
www.cisco.com

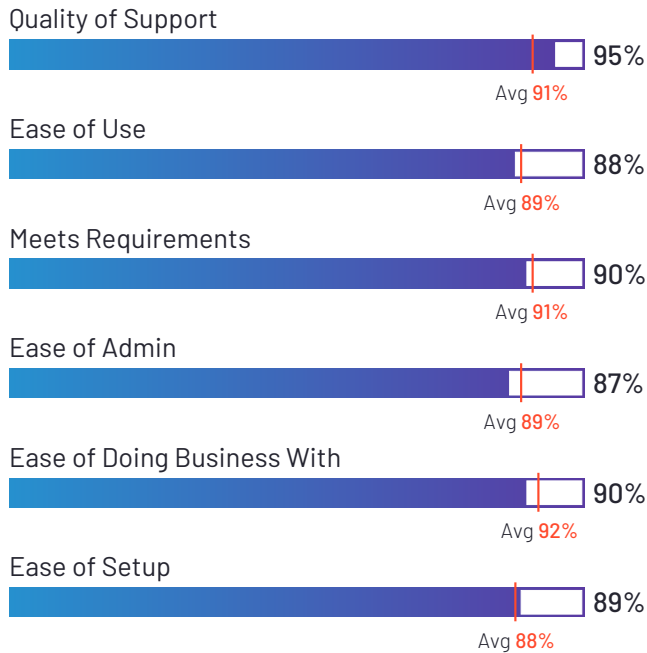


Logpoint

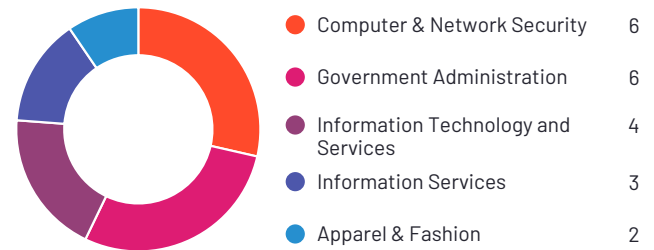
4.3 ★★★★★ (97)

Logpoint 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 Logpoint at a rate of 91%. Logpoint is also in the Log Monitoring, Log Analysis, Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), Threat Intelligence, User and Entity Behavior Analytics (UEBA), SAP Security Software, and SAP Store categories.

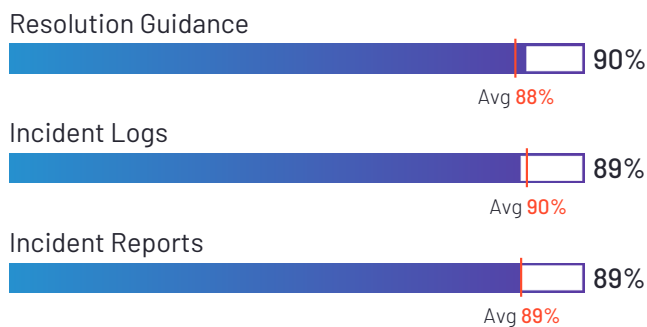
Satisfaction Ratings



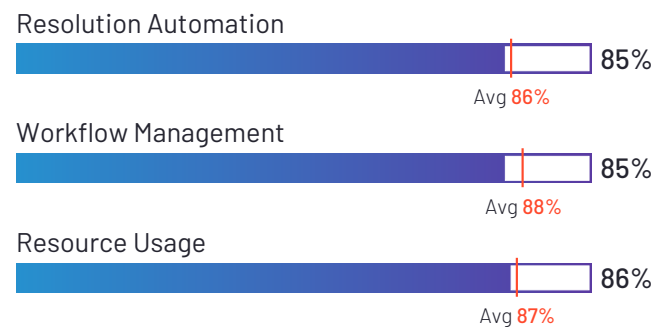
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Logpoint



HQ Location
Copenhagen, Capital Region



Year Founded
2001



Employees (Listed On LinkedIn)
263



Company Website
logpoint.com

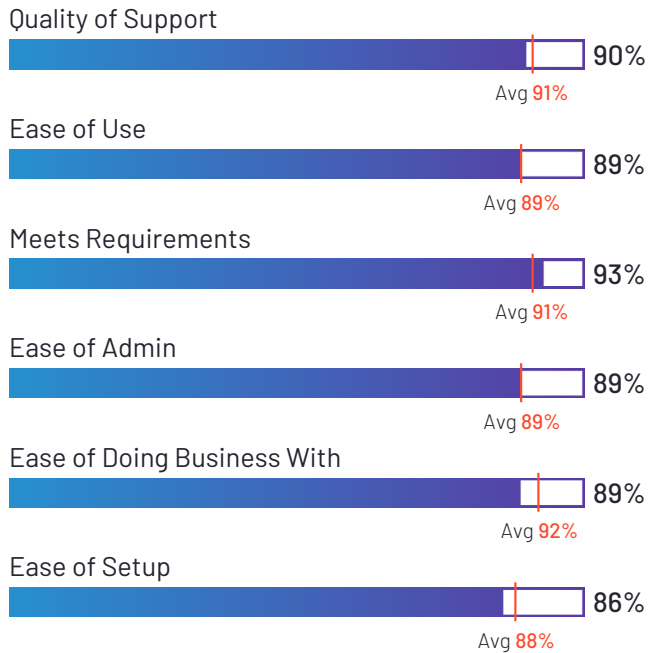


Proofpoint Threat Response Auto-Pull

4.5 ★★★★★ (24)

Proofpoint Threat Response Auto-Pull 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. 92% 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 Proofpoint Threat Response Auto-Pull at a rate of 89%.

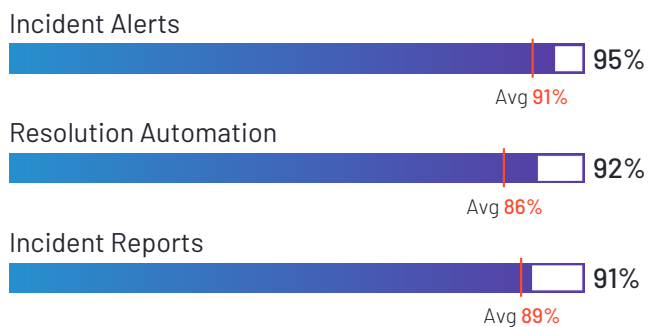
Satisfaction Ratings



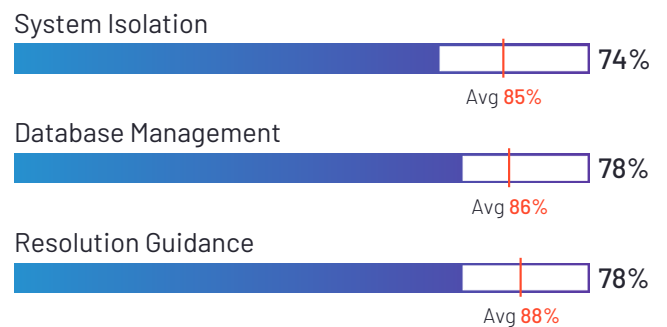
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Proofpoint



HQ Location
Sunnyvale, CA



Year Founded
2002



Employees (Listed On LinkedIn)
4,845



Company Website
proofpoint.com

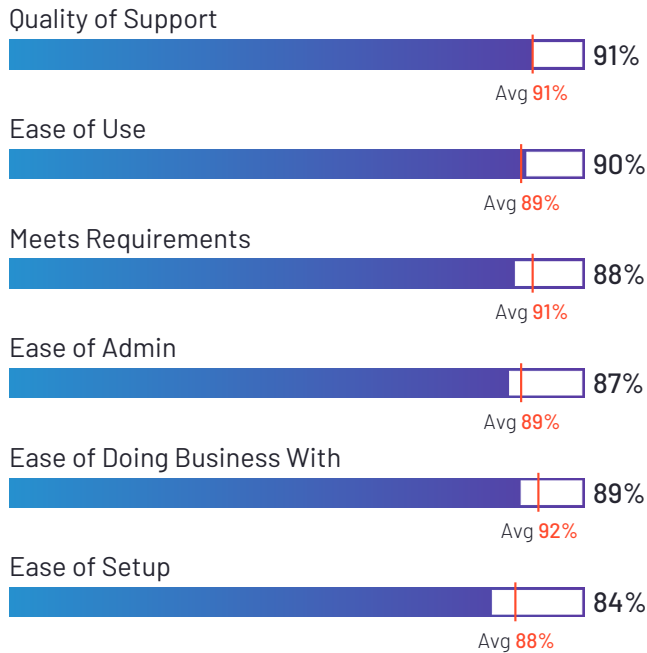


Resolve

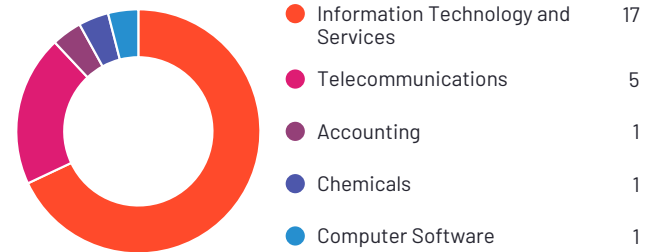
4.5 ★★★★★ (30)

Resolve 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. 93% 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 Resolve at a rate of 89%. Resolve is also in the Cloud Infrastructure Automation, Network Automation Tools, Workload Automation, Robotic Process Automation (RPA), Configuration Management, and Runbook Automation categories.

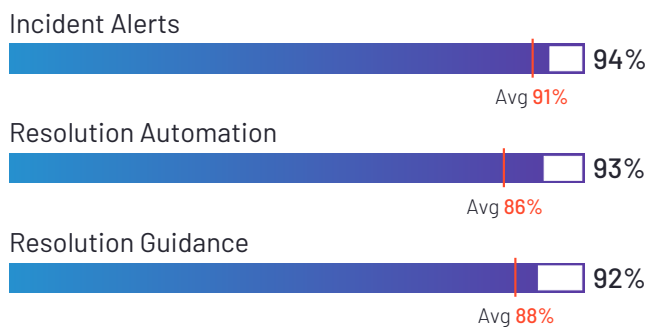
Satisfaction Ratings



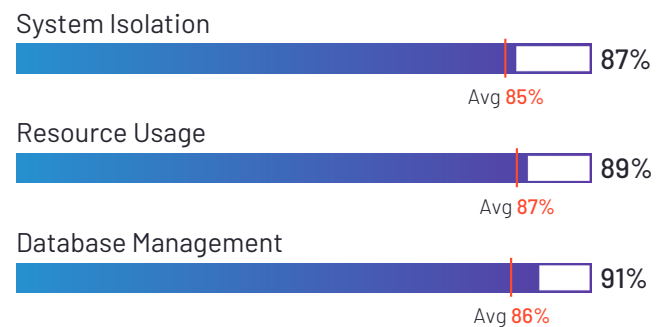
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Resolve



HQ Location
Campbell, California



Year Founded
2014



Employees (Listed On LinkedIn)
103



Company Website
resolve.io

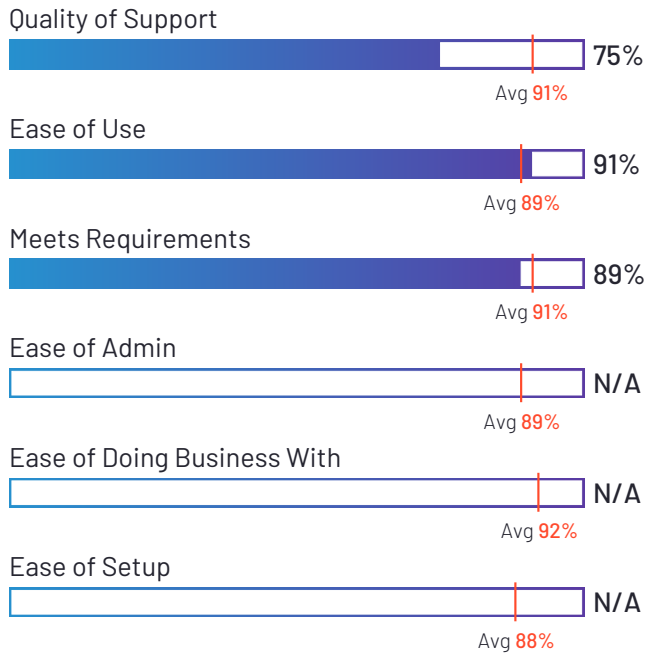


Mozilla Enterprise Defense Platform

4.3 ★★★★★ (10)

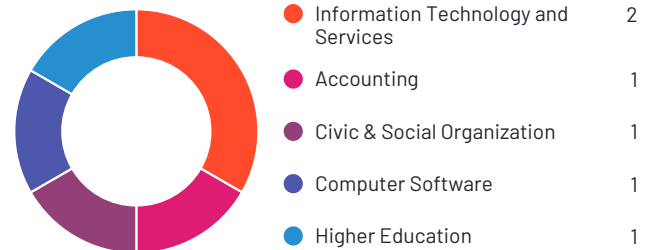
Mozilla Enterprise Defense Platform has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Mozilla Enterprise Defense Platform at a rate of 85%.

Satisfaction Ratings

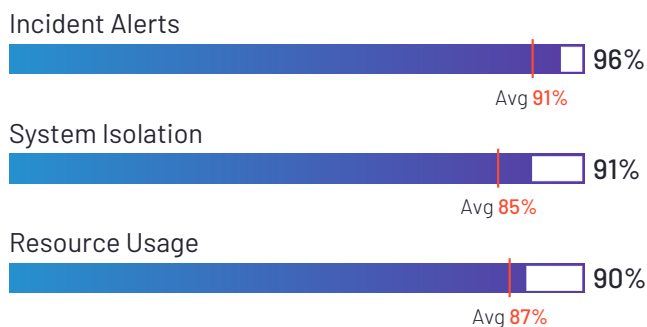


*N/A is displayed when fewer than five responses were received for the question.

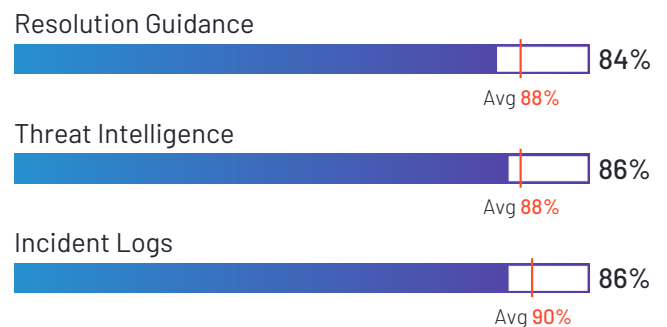
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Mozilla



HQ Location
San Francisco, CA



Year Founded
2005



Employees (Listed On LinkedIn)
1,774



Company Website
mozilla.org

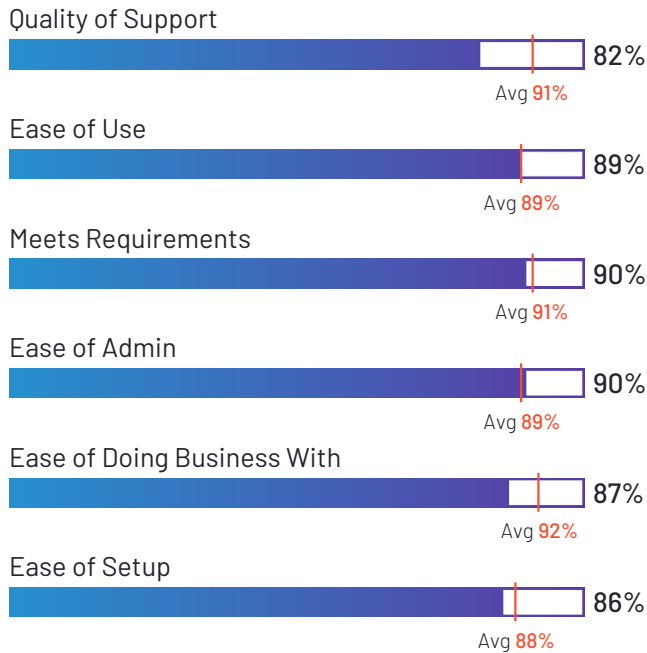


TheHive

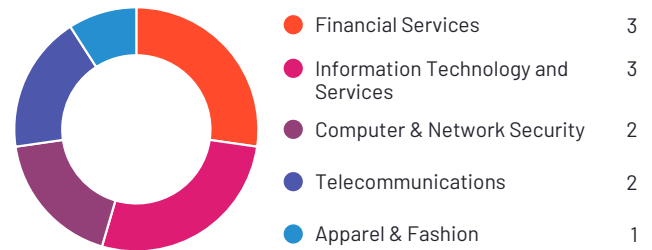
4.2 ★★★★★ (19)

TheHive 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, 88% of users believe it is headed in the right direction, and users said they would be likely to recommend TheHive at a rate of 85%.

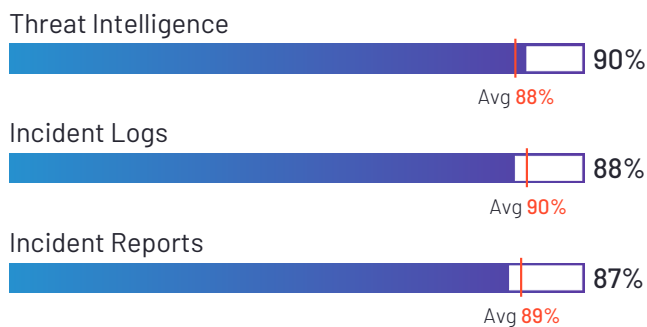
Satisfaction Ratings



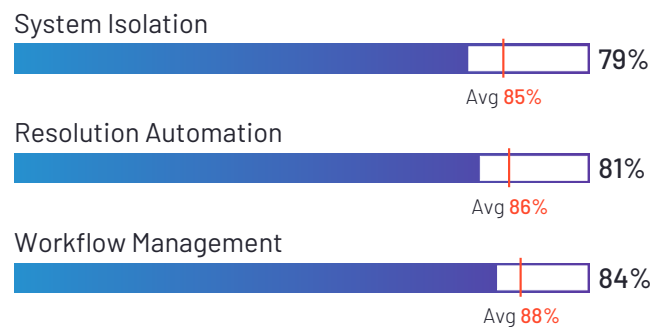
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
TheHive



HQ Location
Paris, FR



Year Founded
2018



Employees (Listed On LinkedIn)
58



Company Website
thehive-project.org

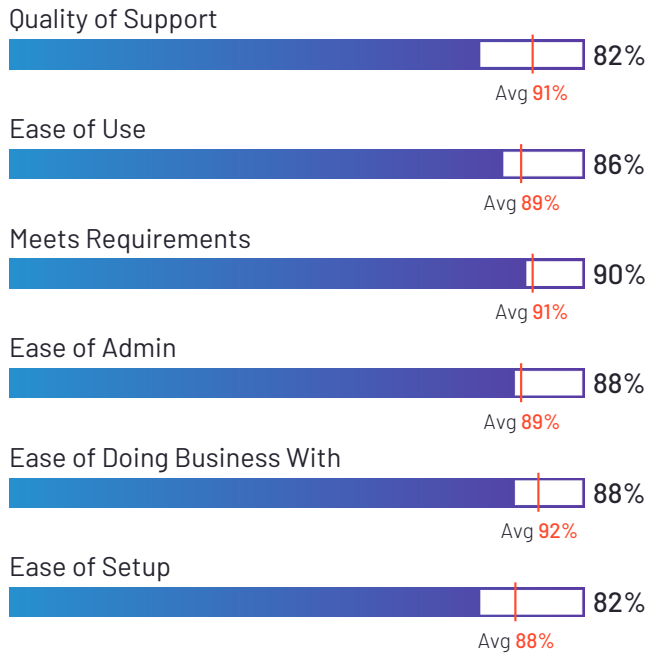


Wazuh - The Open Source Security Platform

4.5 ★★★★★ (60)

Wazuh - The Open Source Security Platform 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, 88% of users believe it is headed in the right direction, and users said they would be likely to recommend Wazuh - The Open Source Security Platform at a rate of 91%. Wazuh - The Open Source Security Platform is also in the Endpoint Detection & Response (EDR) category.

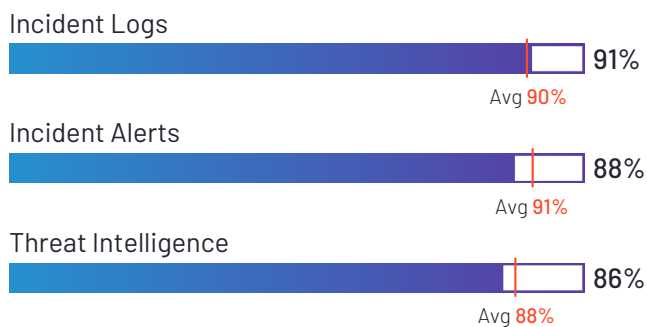
Satisfaction Ratings



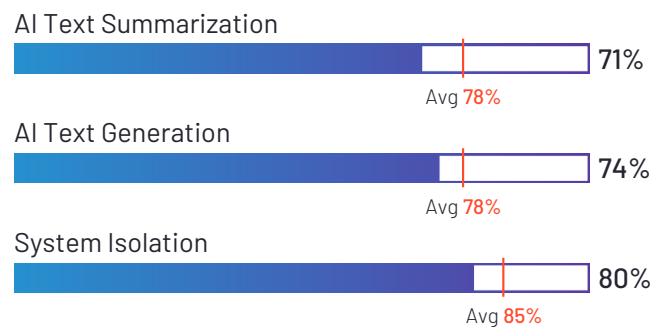
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Wazuh Inc.



HQ Location
Campbell, US



Year Founded
2015



Employees (Listed On LinkedIn)
254



Company Website
wazuh.com

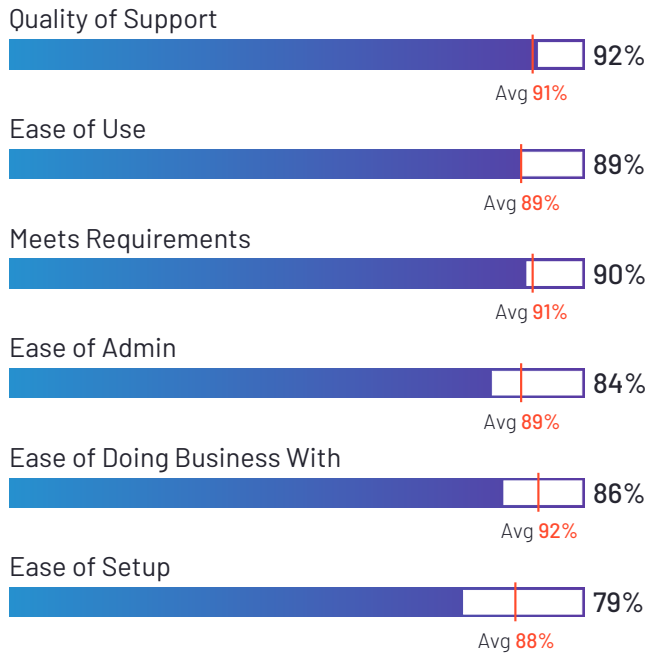


D3 Security

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. 89% 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 D3 Security at a rate of 84%. D3 Security is also in the Security Orchestration, Automation, and Response (SOAR) and Protective Intelligence Platforms categories.

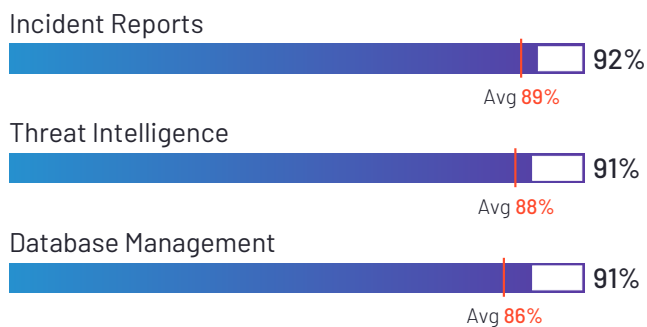
Satisfaction Ratings



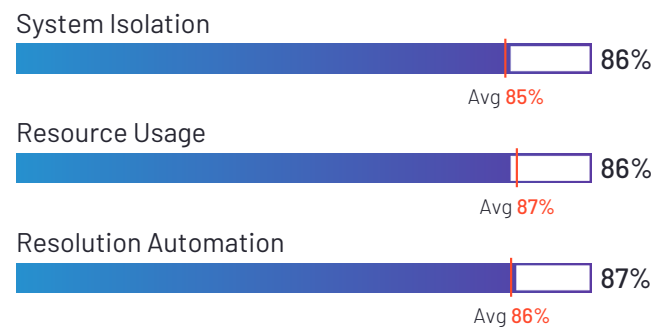
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
D3 Security
Management
Systems



HQ Location
Vancouver, British
Columbia



Year Founded
2012



**Employees (Listed
On LinkedIn)**
173



Company Website
d3security.com

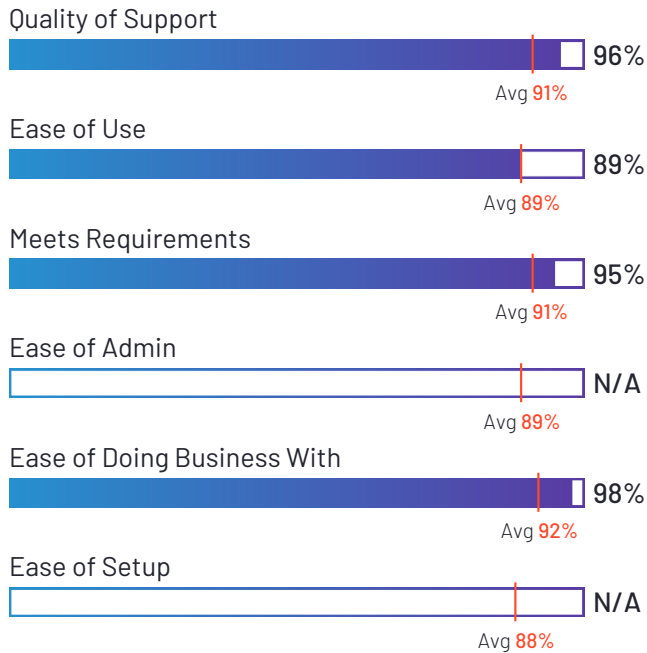


Activu vis|ability

4.7 ★★★★★ (12)

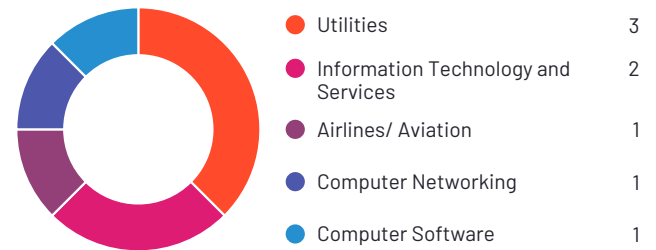
Activu vis|ability has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Activu vis|ability at a rate of 94%.

Satisfaction Ratings



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

Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Activu



HQ Location
Rockaway, US



Year Founded
1983



**Employees (Listed
On LinkedIn)**
88



Company Website
activu.com

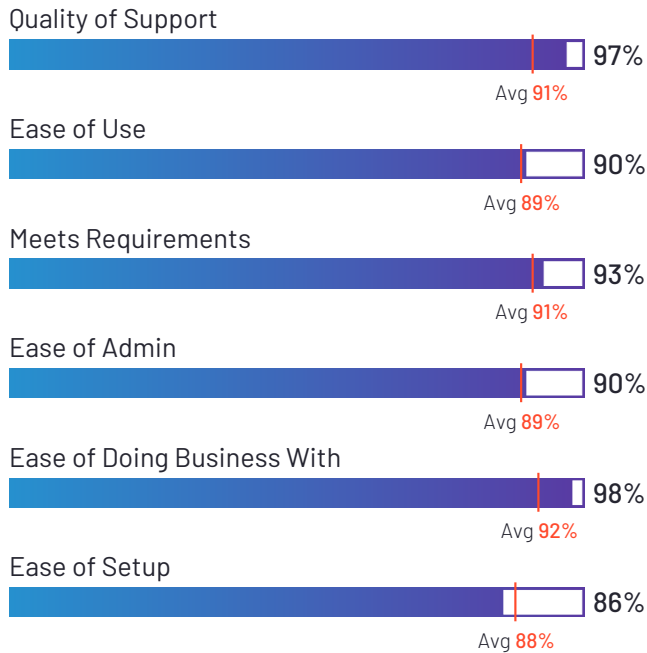


DERDACK Enterprise Alert

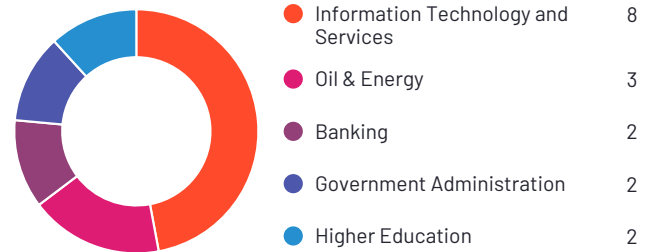
4.8 ★★★★★ (49)

DERDACK Enterprise Alert 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 DERDACK Enterprise Alert at a rate of 97%. DERDACK Enterprise Alert is also in the Incident Management and IT Alerting categories.

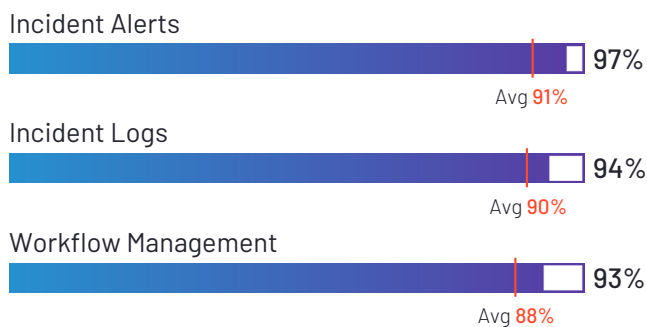
Satisfaction Ratings



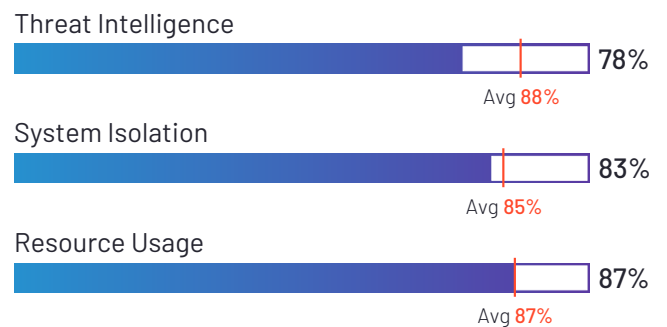
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Derdack



HQ Location
Potsdam, Germany



Year Founded
1999



Employees (Listed On LinkedIn)
32



Company Website
derdack.com

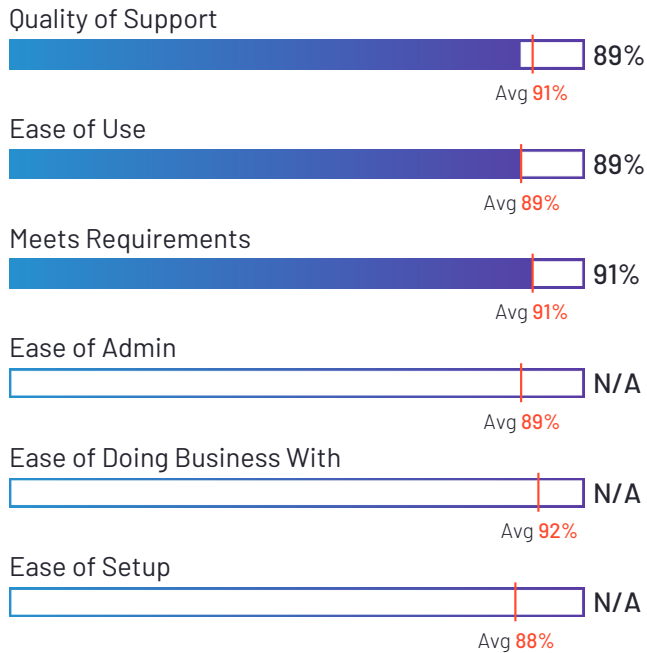


Cyber Triage

4.4 ★★★★★ (17)

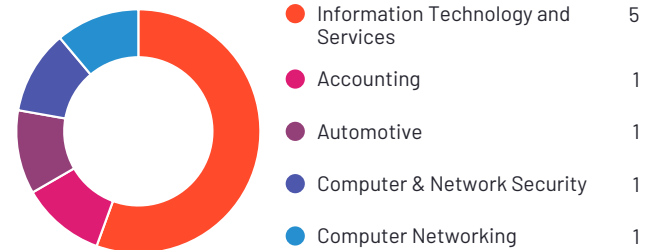
Cyber Triage has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 93% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Cyber Triage at a rate of 87%. Cyber Triage is also in the Digital Forensics category.

Satisfaction Ratings

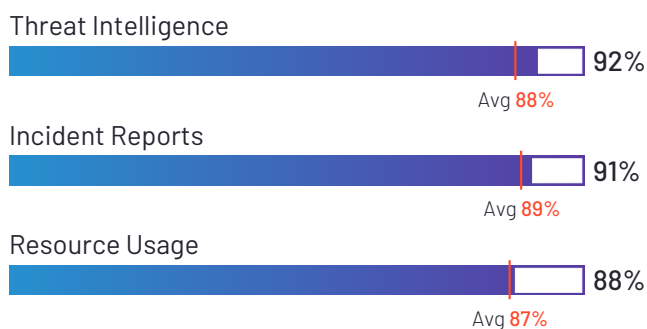


*N/A is displayed when fewer than five responses were received for the question.

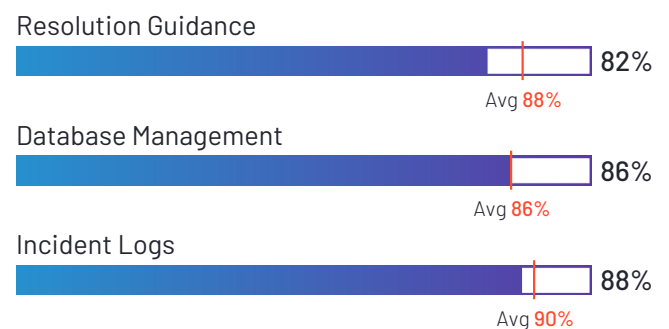
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Basis Technology



HQ Location
Somerville, US



Year Founded
1995



Employees (Listed On LinkedIn)
57



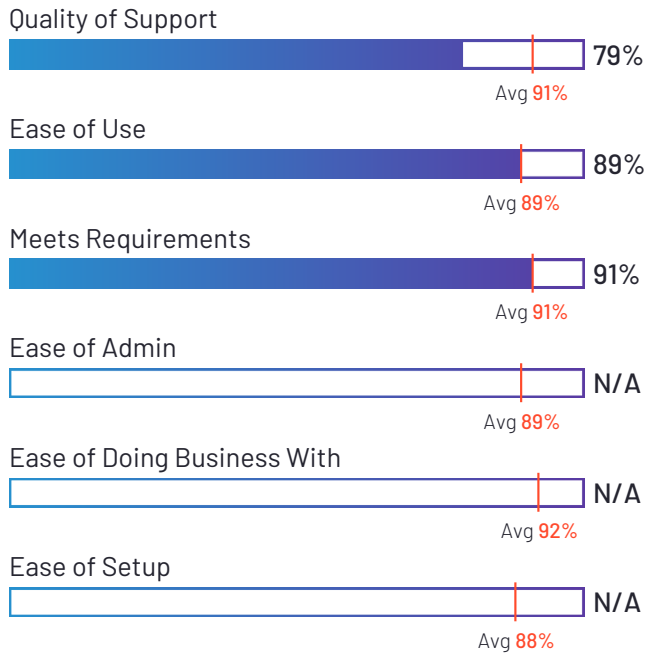
Company Website
basistech.com

ASGARD Mangement System

4.3 ★★★★★ (14)

ASGARD Mangement System 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, 78% of users believe it is headed in the right direction, and users said they would be likely to recommend ASGARD Mangement System at a rate of 86%.

Satisfaction Ratings

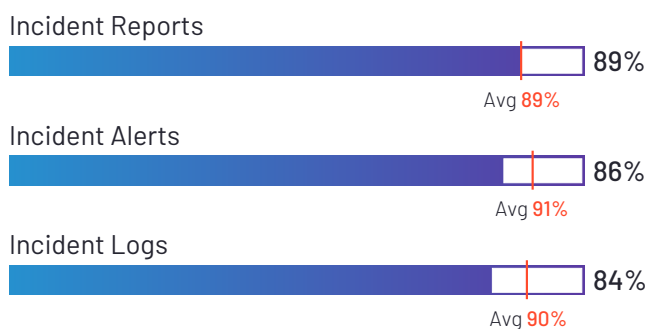


*N/A is displayed when fewer than five responses were received for the question.

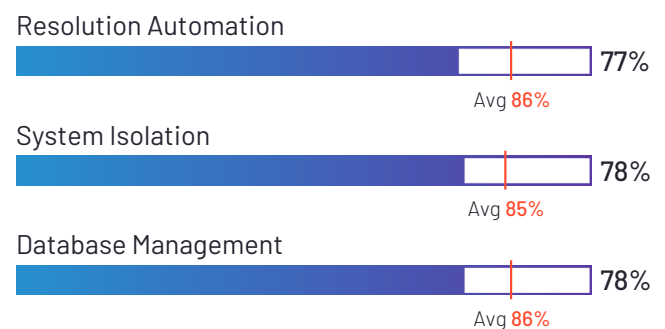
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Nextron Systems



HQ Location
Dietzenbach, Hessen



Year Founded
2017



Employees (Listed On LinkedIn)
46



Company Website
nextron-systems.com

Satisfaction Ratings for Incident Response

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	91%	94%	91%	91%	95%	94%	87%	90%	74
Datadog	89%	95%	92%	85%	89%	88%	83%	86%	64
IBM Instana	82%	84%	84%	83%	82%	85%	94%	86%	42
Dynatrace	92%	92%	90%	88%	90%	91%	86%	86%	75
Tines	96%	96%	93%	94%	99%	97%	94%	95%	89
ServiceNow Security Operations	88%	90%	94%	81%	89%	91%	81%	83%	52
Torq	96%	100%	96%	96%	100%	95%	94%	93%	93
Cynet - All-in-One Cybersecurity Platform	95%	96%	94%	94%	97%	93%	95%	93%	89
CYREBRO	87%	90%	86%	91%	89%	86%	84%	89%	54
Resolver	88%	87%	85%	75%	91%	93%	76%	81%	54
AlienVault USM (from AT&T Cybersecurity)	91%	88%	93%	85%	91%	91%	81%	88%	71
SpinOne	97%	100%	98%	93%	97%	98%	95%	90%	93
Barracuda Incident Response	90%	91%	92%	96%	91%	94%	96%	96%	69
UnderDefense MAXI	95%	100%	97%	94%	98%	100%	94%	96%	84
Blumira Automated Detection & Response	95%	100%	92%	94%	97%	97%	94%	93%	85
Splunk On-Call	95%	93%	95%	91%	100%	94%	94%	91%	80
Defendify All-In-One Cybersecurity Solution	96%	94%	93%	98%	99%	98%	94%	94%	92

(Satisfaction Ratings for Incident Response 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 Incident Response (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	
Intezer	89%	92%	88%	90%	86%	92%	98%	92%	64
SIRP	94%	90%	96%	100%	100%	99%	98%	96%	81
Palo Alto Cortex XSIAM	87%	89%	87%	84%	88%	85%	83%	85%	54
Sumo Logic	88%	88%	91%	88%	87%	89%	87%	84%	63
OneTrust Tech Risk & Compliance	94%	93%	93%	96%	97%	97%	92%	91%	82
InsightIDR	88%	89%	90%	87%	87%	90%	86%	91%	59
Proofpoint Threat Defense	91%	86%	89%	93%	93%	89%	95%	89%	75
Darktrace/Network	89%	91%	94%	73%	93%	93%	88%	73%	68
LogRhythm SIEM	87%	89%	88%	83%	90%	88%	83%	88%	54
Splunk SOAR (Security Orchestration, Automation and Response)	88%	83%	88%	84%	90%	91%	82%	84%	54
Splunk Synthetic Monitoring	90%	100%	93%	N/A	N/A	95%	N/A	93%	75
Logpoint	91%	100%	90%	87%	90%	95%	89%	88%	70
Proofpoint Threat Response Auto-Pull	89%	95%	93%	89%	89%	90%	86%	89%	62
Resolve	89%	96%	88%	87%	89%	91%	84%	90%	59
Mozilla Enterprise Defense Platform	85%	100%	89%	N/A	N/A	75%	N/A	91%	50
TheHive	85%	88%	90%	90%	87%	82%	86%	89%	42
Wazuh - The Open Source Security Platform	91%	88%	90%	88%	88%	82%	82%	86%	67

(Satisfaction Ratings for Incident Response 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 Incident Response (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	
D3 Security	84%	92%	90%	84%	86%	92%	79%	89%	39
Activu vislability	94%	100%	95%	N/A	98%	96%	N/A	89%	83
DERDACK Enterprise Alert	97%	100%	93%	90%	98%	97%	86%	90%	93
Cyber Triage	87%	100%	91%	N/A	N/A	89%	N/A	89%	53
ASGARD Mangement System	86%	78%	91%	N/A	N/A	79%	N/A	89%	69
Average	90%	93%	91%	89%	92%	91%	88%	89%	69

*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 Incident Response

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

	Resolution Automation	Resolution Guidance	System Isolation	Threat Intelligence
KnowBe4 PhishER/PhishER Plus	86%	85%		87%
Datadog				82%
IBM Instana	89%	89%	83%	N/A
Dynatrace	79%	84%	74%	81%
Tines		93%	79%	86%
ServiceNow Security Operations	90%	90%	90%	90%
Torq	91%	90%	85%	90%
Cynet - All-in-One Cybersecurity Platform	94%	94%	91%	92%
CYREBRO	84%	86%	77%	88%
Resolver	69%	75%	71%	66%
AlienVault USM (from AT&T Cybersecurity)	88%	90%	92%	93%
SpinOne	90%	91%	93%	93%
Barracuda Incident Response	89%	90%	93%	89%
UnderDefense MAXI	95%	97%	91%	98%
Blumira Automated Detection & Response	87%	94%	86%	92%
Splunk On-Call	N/A	N/A	N/A	N/A
Defendify All-In-One Cybersecurity Solution	N/A	93%	N/A	93%

(Feature Comparison for Incident Response 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 Incident Response (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

	Resolution Automation	Resolution Guidance	System Isolation	Threat Intelligence
Intezer	N/A	N/A		N/A
SIRP	91%	97%	96%	98%
Palo Alto Cortex XSIAM	81%	82%	79%	85%
Sumo Logic	80%	85%	78%	80%
OneTrust Tech Risk & Compliance	N/A	N/A	N/A	N/A
InsightIDR	88%	89%	88%	93%
Proofpoint Threat Defense	84%	86%	81%	86%
Darktrace/Network	90%	90%	100%	86%
LogRhythm SIEM	84%	86%	83%	89%
Splunk SOAR (Security Orchestration, Automation and Response)	88%	87%	85%	90%
Splunk Synthetic Monitoring	84%	92%	89%	84%
Logpoint	85%	90%	88%	87%
Proofpoint Threat Response Auto-Pull	92%	78%	74%	86%
Resolve	93%	92%	87%	91%
Mozilla Enterprise Defense Platform	88%	84%	91%	86%
TheHive	81%	84%	79%	90%
Wazuh - The Open Source Security Platform	81%	81%	80%	86%

(Feature Comparison for Incident Response 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 Incident Response (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

	Resolution Automation	Resolution Guidance	System Isolation	Threat Intelligence
D3 Security	87%		86%	91%
Activu vislability	89%	89%	N/A	N/A
DERDACK Enterprise Alert	89%	90%	83%	78%
Cyber Triage		82%		92%
ASGARD Mangement System	77%	80%	78%	84%
Average	86%	88%	85%	88%

(Feature Comparison for Incident Response 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 Incident Response (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.

Records

	Incident Logs	Incident Reports	Resource Usage
KnowBe4 PhishER/PhishER Plus	87%	87%	84%
Datadog	93%	91%	87%
IBM Instana	N/A	N/A	N/A
Dynatrace	88%	86%	90%
Tines	93%	88%	88%
ServiceNow Security Operations	91%	89%	90%
Torq	82%	82%	83%
Cynet - All-in-One Cybersecurity Platform	92%	92%	90%
CYREBRO	88%	85%	84%
Resolver	86%	82%	77%
AlienVault USM (from AT&T Cybersecurity)	93%	93%	92%
SpinOne	95%	95%	94%
Barracuda Incident Response	88%	88%	86%
UnderDefense MAXI	100%	99%	96%
Blumira Automated Detection & Response	91%	89%	91%
Splunk On-Call	N/A	N/A	N/A
Defendify All-In-One Cybersecurity Solution	N/A	92%	94%

(Feature Comparison for Incident Response 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 Incident Response (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.

Records

	Incident Logs	Incident Reports	Resource Usage
Intezer	N/A	N/A	N/A
SIRP	96%	96%	91%
Palo Alto Cortex XSIAM	89%	86%	84%
Sumo Logic	90%	86%	85%
OneTrust Tech Risk & Compliance	91%	91%	91%
InsightIDR	93%	91%	86%
Proofpoint Threat Defense	87%	89%	83%
Darktrace/Network	86%	91%	74%
LogRhythm SIEM	90%	90%	90%
Splunk SOAR (Security Orchestration, Automation and Response)	90%	92%	84%
Splunk Synthetic Monitoring	92%	90%	78%
Logpoint	89%	89%	86%
Proofpoint Threat Response Auto-Pull	88%	91%	
Resolve	N/A	N/A	89%
Mozilla Enterprise Defense Platform	86%	88%	90%
TheHive	88%	87%	84%
Wazuh - The Open Source Security Platform	91%	83%	82%

(Feature Comparison for Incident Response 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 Incident Response (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.

Records

	Incident Logs	Incident Reports	Resource Usage
D3 Security		92%	86%
Activu vislability	N/A	N/A	N/A
DERDACK Enterprise Alert	94%	88%	87%
Cyber Triage	88%	91%	88%
ASGARD Mangement System	84%	89%	79%
Average	90%	89%	86%

(Feature Comparison for Incident Response 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 Incident Response (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.

Management

	Incident Alerts	Database Management	Workflow Management
KnowBe4 PhishER/PhishER Plus	88%	82%	87%
Datadog	93%	86%	
IBM Instana	N/A	N/A	N/A
Dynatrace	90%	85%	86%
Tines	94%	86%	93%
ServiceNow Security Operations	92%	90%	94%
Torq	96%	81%	96%
Cynet - All-in-One Cybersecurity Platform	95%	91%	91%
CYREBRO	90%	83%	84%
Resolver	80%	83%	85%
AlienVault USM (from AT&T Cybersecurity)	95%	86%	90%
SpinOne	94%	94%	94%
Barracuda Incident Response	89%	88%	88%
UnderDefense MAXI	99%	94%	96%
Blumira Automated Detection & Response	94%	83%	88%
Splunk On-Call	N/A	N/A	N/A
Defendify All-In-One Cybersecurity Solution	93%	N/A	N/A

(Feature Comparison for Incident Response 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 Incident Response (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.

Management

	Incident Alerts	Database Management	Workflow Management
Intezer	N/A	N/A	
SIRP	95%	90%	94%
Palo Alto Cortex XSIAM	88%	84%	85%
Sumo Logic	88%	83%	84%
OneTrust Tech Risk & Compliance	N/A	N/A	N/A
InsightIDR	91%	89%	88%
Proofpoint Threat Defense	89%	86%	93%
Darktrace/Network	89%	80%	80%
LogRhythm SIEM	90%	89%	88%
Splunk SOAR (Security Orchestration, Automation and Response)	90%	83%	87%
Splunk Synthetic Monitoring	89%	84%	81%
Logpoint	88%	86%	85%
Proofpoint Threat Response Auto-Pull	95%	78%	78%
Resolve	94%	91%	N/A
Mozilla Enterprise Defense Platform	96%	88%	88%
TheHive	86%	86%	84%
Wazuh - The Open Source Security Platform	88%	81%	81%

(Feature Comparison for Incident Response 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 Incident Response (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.

Management

	Incident Alerts	Database Management	Workflow Management
D3 Security		91%	91%
Activu vislability	N/A	N/A	N/A
DERDACK Enterprise Alert	97%	90%	93%
Cyber Triage		86%	
ASGARD Mangement System	86%	78%	81%
Average	91%	86%	88%

*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 Incident Response

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	11%	74%	15%
Datadog	17%	48%	35%
IBM Instana	14%	54%	32%
Dynatrace	10%	30%	60%
Tines	21%	36%	43%
ServiceNow Security Operations	19%	10%	71%
Torq	31%	40%	29%
Cynet - All-in-One Cybersecurity Platform	37%	51%	12%
CYREBRO	28%	59%	13%
Resolver	12%	29%	59%
AlienVault USM (from AT&T Cybersecurity)	15%	67%	19%
SpinOne	59%	38%	3%
Barracuda Incident Response	23%	54%	23%
UnderDefense MAXI	15%	69%	15%
Blumira Automated Detection & Response	33%	59%	8%
Splunk On-Call	7%	53%	40%
Defendify All-In-One Cybersecurity Solution	82%	18%	0%

(Additional Data for Incident Response continues on next page)

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

Additional Data for Incident Response (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.)
Intezer	53%	24%	24%
SIRP	45%	27%	27%
Palo Alto Cortex XSIAM	17%	27%	55%
Sumo Logic	14%	52%	35%
OneTrust Tech Risk & Compliance	46%	39%	14%
InsightIDR	20%	54%	25%
Proofpoint Threat Defense	25%	50%	25%
Darktrace/Network	6%	88%	6%
LogRhythm SIEM	18%	43%	39%
Splunk SOAR (Security Orchestration, Automation and Response)	21%	46%	33%
Splunk Synthetic Monitoring	50%	25%	25%
Logpoint	23%	48%	30%
Proofpoint Threat Response Auto-Pull	4%	33%	63%
Resolve	17%	50%	33%
Mozilla Enterprise Defense Platform	40%	40%	20%
TheHive	11%	39%	50%
Wazuh - The Open Source Security Platform	40%	40%	20%

(Additional Data for Incident Response continues on next page)

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



Additional Data for Incident Response (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.)
D3 Security	24%	30%	46%
Activu vislability	50%	33%	17%
DERDACK Enterprise Alert	10%	28%	62%
Cyber Triage	40%	13%	47%
ASGARD Mangement System	23%	38%	38%
Average	26%	42%	31%

(Additional Data for Incident Response continues on next page)

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



Additional Data for Incident Response (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%	1.2	79%	14%	3%	4%	75	25
Datadog	92%	8%	2.9	86%	8%	6%	0%	27	15
IBM Instana	90%	10%	3.4	80%	10%	10%	0%	17	24
Dynatrace	61%	39%	2.8	67%	30%	2%	1%	75	24
Tines	91%	9%	1.1	85%	10%	5%	0%	7	16
ServiceNow Security Operations	33%	67%	4.3	40%	20%	20%	20%	N/A	N/A
Torq	100%	0%	1.3	75%	17%	0%	8%	7	18
Cynet - All-in-One Cybersecurity Platform	87%	13%	1.1	74%	12%	4%	11%	17	18
CYREBRO	72%	28%	1.8	58%	26%	5%	11%	3	18
Resolver	83%	17%	6.4	57%	32%	0%	11%	125	24
AlienVault USM (from AT&T Cybersecurity)	50%	50%	1.6	75%	19%	6%	0%	3	16
SpinOne	88%	13%	0.4	63%	8%	8%	21%	12	14
Barracuda Incident Response	75%	25%	4.5	75%	0%	0%	25%	3	8
UnderDefense MAXI	80%	20%	N/A	80%	20%	0%	0%	N/A	N/A
Blumira Automated Detection & Response	85%	15%	0.5	83%	8%	3%	8%	3	10
Splunk On-Call	90%	10%	1.0	82%	0%	0%	18%	27	9
Defendify All-In-One Cybersecurity Solution	80%	20%	0.3	90%	0%	0%	10%	N/A	10

(Additional Data for Incident Response continues on next page)

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



Additional Data for Incident Response (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)
Intezer	33%	67%	N/A	80%	0%	0%	20%	N/A	N/A
SIRP	63%	38%	0.9	0%	100%	0%	0%	17	14
Palo Alto Cortex XSIAM	30%	70%	3.4	50%	30%	9%	10%	17	24
Sumo Logic	76%	24%	1.6	74%	12%	3%	12%	17	13
OneTrust Tech Risk & Compliance	67%	33%	2.2	89%	0%	0%	11%	N/A	N/A
InsightIDR	87%	13%	3.7	64%	7%	14%	14%	7	13
Proofpoint Threat Defense	80%	20%	1.0	33%	50%	0%	17%	17	19
Darktrace/Network	30%	70%	1.8	0%	100%	0%	0%	7	33
LogRhythm SIEM	27%	73%	2.4	32%	37%	14%	17%	7	22
Splunk SOAR (Security Orchestration, Automation and Response)	43%	57%	N/A	60%	20%	20%	0%	N/A	N/A
Splunk Synthetic Monitoring	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Logpoint	5%	95%	1.8	45%	20%	10%	25%	7	15
Proofpoint Threat Response Auto-Pull	21%	79%	1.0	39%	56%	0%	6%	191	15
Resolve	22%	78%	5.7	88%	13%	0%	0%	225	N/A
Mozilla Enterprise Defense Platform	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
TheHive	38%	62%	2.7	89%	11%	0%	0%	27	10
Wazuh - The Open Source Security Platform	50%	50%	1.0	83%	8%	8%	0%	3	3

(Additional Data for Incident Response continues on next page)

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



Additional Data for Incident Response (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)
D3 Security	20%	80%	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Activu visibility	N/A	N/A	N/A	0%	60%	40%	0%	N/A	N/A
DERDACK Enterprise Alert	32%	68%	2.8	82%	12%	6%	0%	75	14
Cyber Triage	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
ASGARD Mangement System	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

(Additional Data for Incident Response continues on next page)

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

Additional Data for Incident Response (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	77%	12
Datadog	62%	10
IBM Instana	60%	11
Dynatrace	53%	20
Tines	65%	6
ServiceNow Security Operations	N/A	19
Torq	39%	4
Cynet - All-in-One Cybersecurity Platform	84%	13
CYREBRO	75%	15
Resolver	73%	16
AlienVault USM (from AT&T Cybersecurity)	83%	20
SpinOne	80%	12
Barracuda Incident Response	77%	28
UnderDefense MAXI	N/A	N/A
Blumira Automated Detection & Response	65%	12
Splunk On-Call	70%	16
Defendify All-In-One Cybersecurity Solution	74%	14

(Additional Data for Incident Response continues on next page)

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

Additional Data for Incident Response (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)
Intezer	N/A	N/A
SIRP	75%	N/A
Palo Alto Cortex XSIAM	65%	22
Sumo Logic	56%	11
OneTrust Tech Risk & Compliance	59%	N/A
InsightIDR	77%	12
Proofpoint Threat Defense	64%	13
Darktrace/Network	69%	9
LogRhythm SIEM	62%	16
Splunk SOAR (Security Orchestration, Automation and Response)	N/A	N/A
Splunk Synthetic Monitoring	N/A	N/A
Logpoint	53%	23
Proofpoint Threat Response Auto-Pull	91%	18
Resolve	53%	N/A
Mozilla Enterprise Defense Platform	N/A	N/A
TheHive	84%	23
Wazuh - The Open Source Security Platform	43%	11

(Additional Data for Incident Response continues on next page)

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



Additional Data for Incident Response (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)
D3 Security	N/A	N/A
Activu visibility	N/A	N/A
DERDACK Enterprise Alert	67%	12
Cyber Triage	N/A	N/A
ASGARD Mangement System	N/A	N/A
Average	68%	15

(Additional Data for Incident Response continues on next page)

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



Additional Data for Incident Response (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	2,177	310,052
Datadog	Datadog	2010	9,496	434,739
IBM Instana	IBM	1911	328,966	18,000,000
Dynatrace	Dynatrace	2005	5,533	373,166
Tines	Tines	2018	456	49,854
ServiceNow Security Operations	ServiceNow	2004	32,224	1,274,096
Torq	torq	2020	318	27,719
Cynet - All-in-One Cybersecurity Platform	Cynet	2014	287	27,871
CYREBRO	CYREBRO	2013	100	11,848
Resolver	Resolver		748	30,376
AlienVault USM (from AT&T Cybersecurity)	LevelBlue	1876	387	110,362
SpinOne	SpinAI	2017	91	3,382
Barracuda Incident Response	Barracuda	2002	2,158	73,491
UnderDefense MAXI	UnderDefense	2017	119	5,855
Blumira Automated Detection & Response	Blumira	2018	65	7,301
Splunk On-Call	Cisco	1984	94,810	6,861,841
Defendify All-In-One Cybersecurity Solution	Defendify	2017	36	2,364

(Additional Data for Incident Response continues on next page)

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

Additional Data for Incident Response (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
Intezer	Intezer	2015	60	8,977
SIRP	SIRP	2017	52	4,841
Palo Alto Cortex XSIAM	Palo Alto Networks	2005	17,526	1,570,567
Sumo Logic	Sumo Logic	2010	901	159,427
OneTrust Tech Risk & Compliance	OneTrust	2016	2,576	371,904
InsightIDR	Rapid7	2000	3,035	193,890
Proofpoint Threat Defense	Proofpoint	2002	4,845	168,847
Darktrace/Network	Darktrace	2013	2,575	230,396
LogRhythm SIEM	Exabeam	2013	907	46,259
Splunk SOAR (Security Orchestration, Automation and Response)	Cisco	1984	94,810	6,861,841
Splunk Synthetic Monitoring	Cisco	1984	94,810	6,861,841
Logpoint	Logpoint	2001	263	28,586
Proofpoint Threat Response Auto-Pull	Proofpoint	2002	4,845	168,847
Resolve	Resolve	2014	103	19,382
Mozilla Enterprise Defense Platform	Mozilla	2005	1,774	425,759
TheHive	TheHive	2018	58	7,004
Wazuh - The Open Source Security Platform	Wazuh Inc.	2015	254	61,336

(Additional Data for Incident Response continues on next page)

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



Additional Data for Incident Response (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
D3 Security	D3 Security Management Systems	2012	173	19,612
Activu vislability	Activu	1983	88	2,741
DERDACK Enterprise Alert	Derdack	1999	32	677
Cyber Triage	Basis Technology	1995	57	9,687
ASGARD Mangement System	Nextron Systems	2017	46	3,952

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