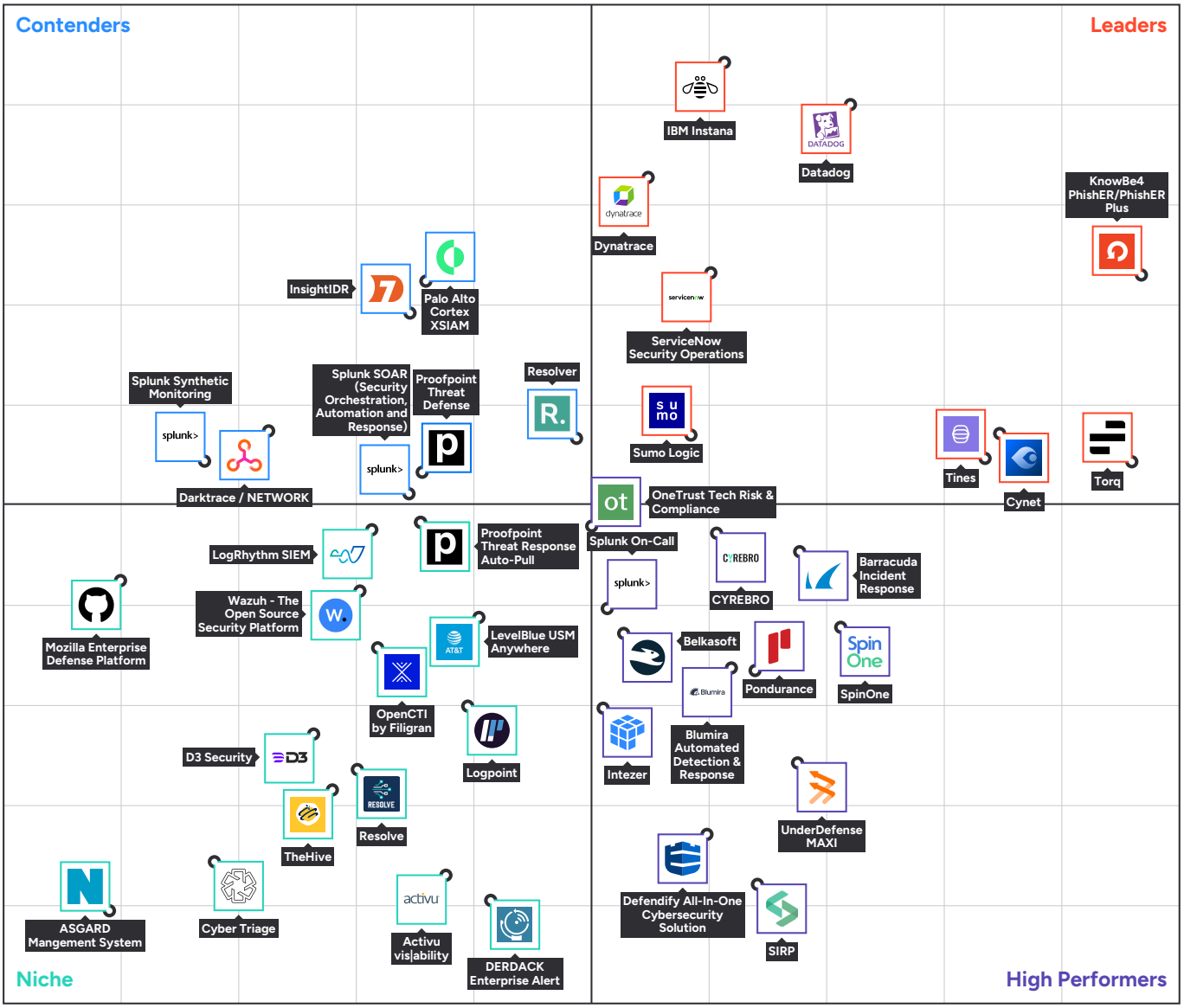
Grid® Report for Incident Response
Spring 2026

Incident Response Software



(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 February 17, 2026. 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, Torq, Cynet, Dynatrace, Tines, ServiceNow Security Operations, and Sumo Logic
- High Performing products have high customer Satisfaction scores and low Market Presence compared to the rest of the category. High Performers include: Barracuda Incident Response, SpinOne, CYREBRO, OneTrust Tech Risk & Compliance, Pondurance, Blumira Automated Detection & Response, UnderDefense MAXI, Splunk On-Call, Belkasoft, Intezer, Defendify All-In-One Cybersecurity Solution, 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, Resolver, InsightIDR, Proofpoint Threat Response, Splunk SOAR (Security Orchestration, Automation and Response), Darktrace / NETWORK, 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: Proofpoint Threat Response Auto-Pull, LevelBlue USM Anywhere, LogRhythm SIEM, Wazuh - The Open Source Security Platform, Logpoint, OpenCTI by Filigran, D3 Security, Resolve, Mozilla Enterprise Defense Platform, DERDACK Enterprise Alert, Activu vis|ability, TheHive, 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	440	100	75	88
Datadog	136	74	94	84
IBM Instana	46	62	99	81
Torq	94	99	55	77
Cynet	136	87	58	72
Dynatrace	256	55	86	71
Tines	88	86	55	70
ServiceNow Security Operations	23	61	76	68
Sumo Logic	125	59	58	58

(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.

High Performers

	# of Reviews	Satisfaction	Market Presence	G2 Score
Barracuda Incident Response	15	69	45	57
SpinOne	35	73	36	55
CYREBRO	99	61	47	54
OneTrust Tech Risk & Compliance	28	50	48	49
Pondurance	11	65	32	48
Blumira Automated Detection & Response	65	63	32	47
UnderDefense MAXI	13	69	21	45
Splunk On-Call	15	52	38	45
Belkasoft	19	53	35	44
Intezer	18	51	27	39
Defendify All-In-One Cybersecurity Solution	28	61	13	37
SIRP	22	65	8	36

(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	259	35	75	55
Resolver	78	49	57	53
InsightIDR	62	34	71	52
Proofpoint Threat Defense	16	35	54	44
Splunk SOAR (Security Orchestration, Automation and Response)	24	34	51	42
Darktrace / NETWORK	16	21	58	40
Splunk Synthetic Monitoring	12	15	55	35

(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
Proofpoint Threat Response Auto-Pull	24	35	48	41
LevelBlue USM Anywhere	28	40	37	39
LogRhythm SIEM	95	30	47	39
Wazuh - The Open Source Security Platform	42	29	40	35
Logpoint	45	39	28	33
OpenCTI by Filigran	12	31	34	32
D3 Security	63	25	25	25
Resolve	30	29	21	25
Mozilla Enterprise Defense Platform	10	7	42	24
DERDACK Enterprise Alert	31	41	6	23
Activu vis|ability	12	37	9	23
TheHive	19	27	18	22
Cyber Triage	15	16	10	13
ASGARD Mangement System	13	6	5	6

* 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 | Spring 2026 is based on reviews collected through February 17, 2026. We apply unique algorithms to this data to calculate Satisfaction (v4.0) and Market Presence (v7.0) scores for the Spring 2026 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 February 17, 2026. The ratings may change as the products are further developed, the sellers grow, and as additional opinions are shared by users. G2 updates the ratings on its website in real time as additional data is received, and this report will be updated as significant data is received. By improving their products and support and/or by having more satisfied customer voices heard, Contenders may become Leaders and Niche sellers may become High Performers.

Trust

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

(Grid® Methodology continues on next page)

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

Grid® Methodology (continued)

Grid® Inclusion Criteria

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

If a product is not yet listed on G2 and it fits the market definition above, then users are encouraged to suggest its addition to our Incident Response category.

Product Profiles

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

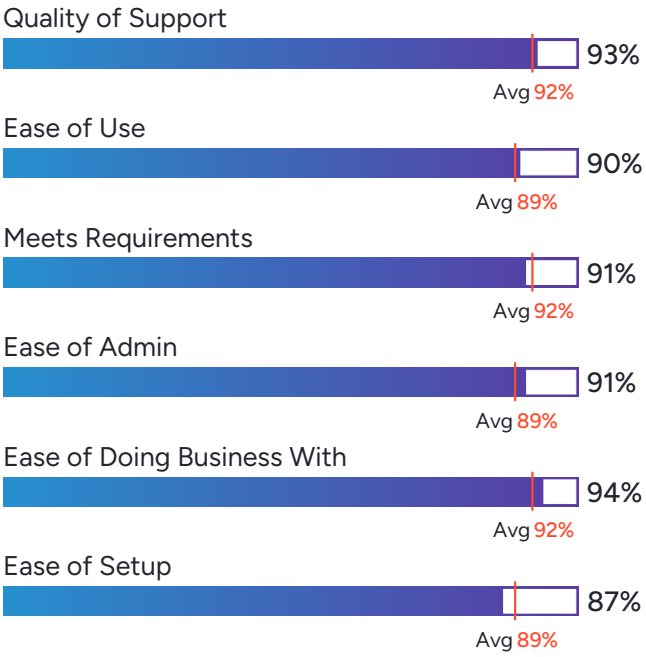
KnowBe4 PhishER/PhishER Plus

4.5 (550)

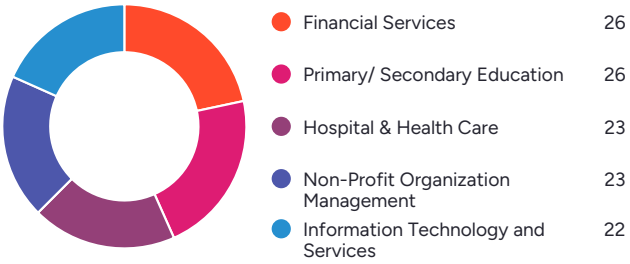
SPRING 2026 Leader

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.

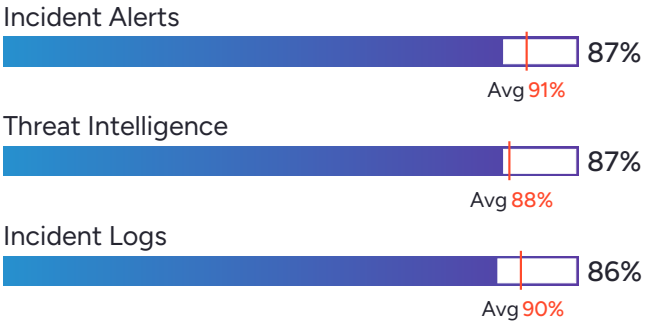
Satisfaction Ratings



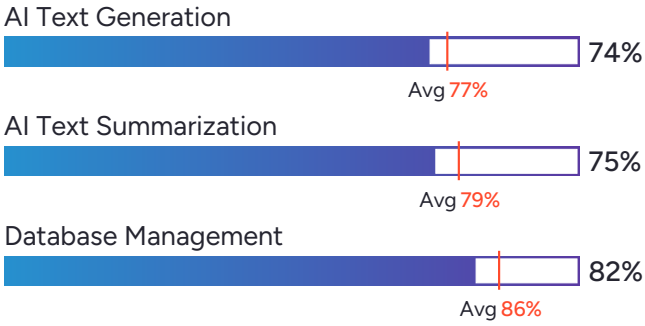
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
KnowBe4, Inc.

HQ Location
Clearwater, FL

Year Founded
2010

Employees (Listed On Linkedin)
2,387

Company Website
knowbe4.com

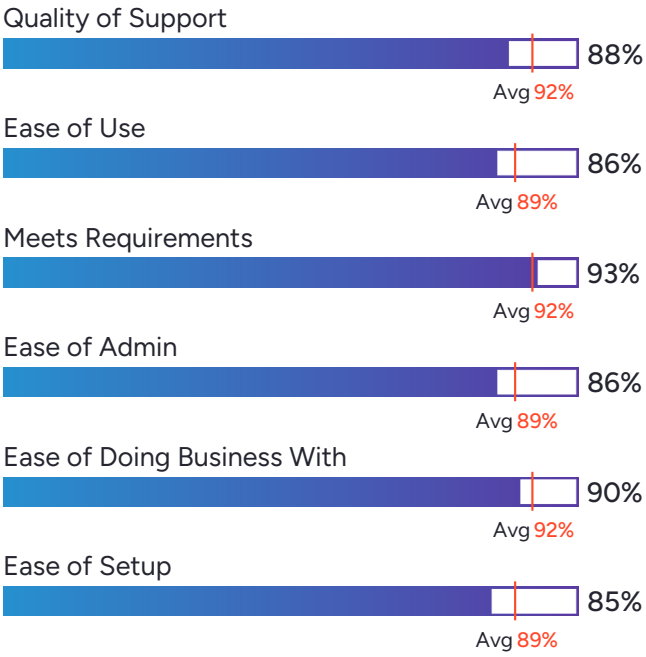
Datadog

4.4 ★★★★½ (690)

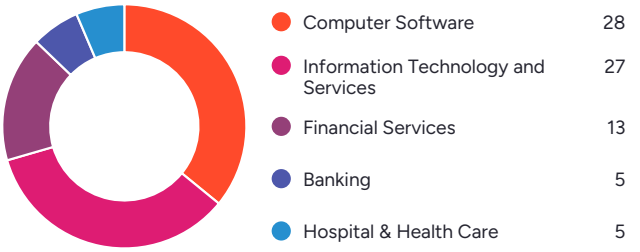
SPRING 2026 Leader

Datadog 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, 96% 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, Cloud Cost Management, and Digital Experience Monitoring (DEM) categories.

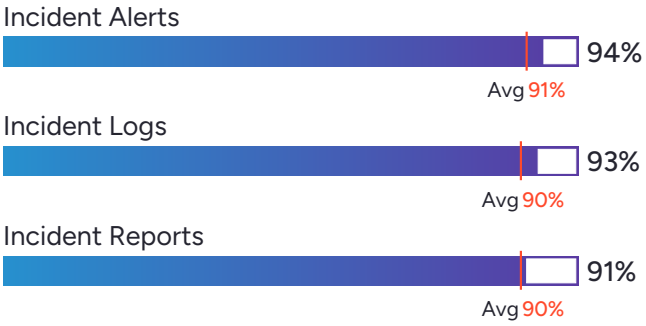
Satisfaction Ratings



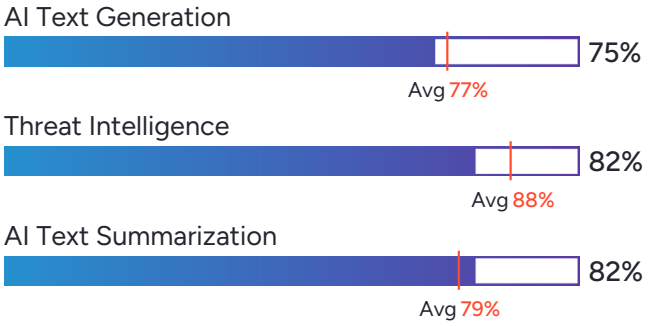
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Datadog

HQ Location
New York

Year Founded
2010

Employees (Listed On Linkedin)
10,625

Company Website
datadoghq.com

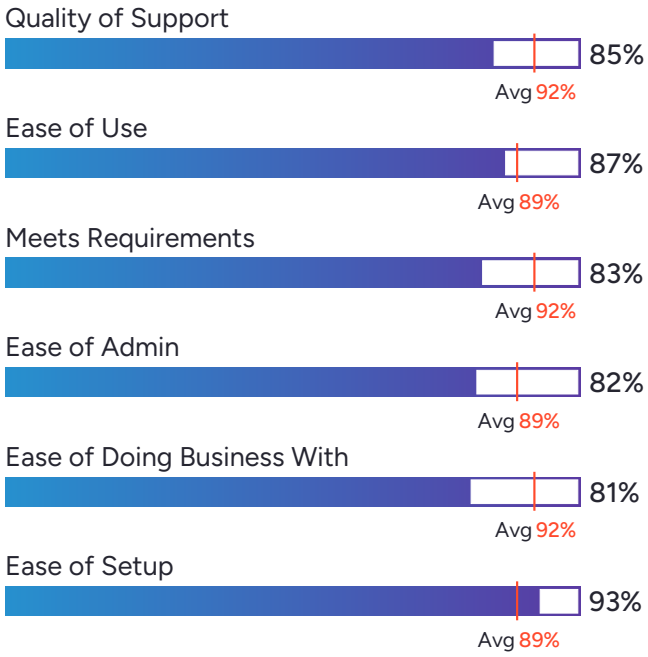
IBM Instana

4.4 ★★★★½ (460)

SPRING 2026 Leader

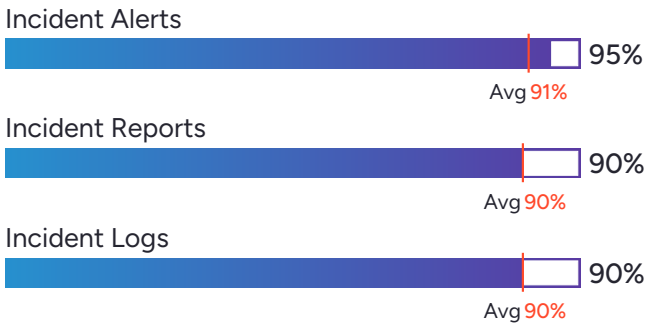
IBM Instana has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. IBM Instana has the largest Market Presence among products in Incident Response. 90% of users rated it 4 or 5 stars, 81% of users believe it is headed in the right direction, and users said they would be likely to recommend IBM Instana at a rate of 85%. 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

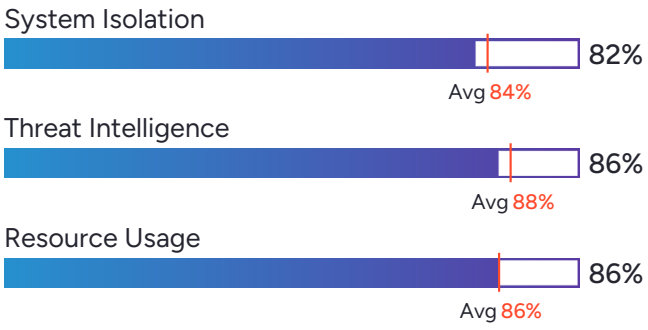


Top Industries Represented

Highest-Rated Features



Lowest-Rated Features



Ownership
IBM

HQ Location
Armonk, NY

Year Founded
1911

Employees (Listed On Linkedin)
339,241

Company Website
www.ibm.com

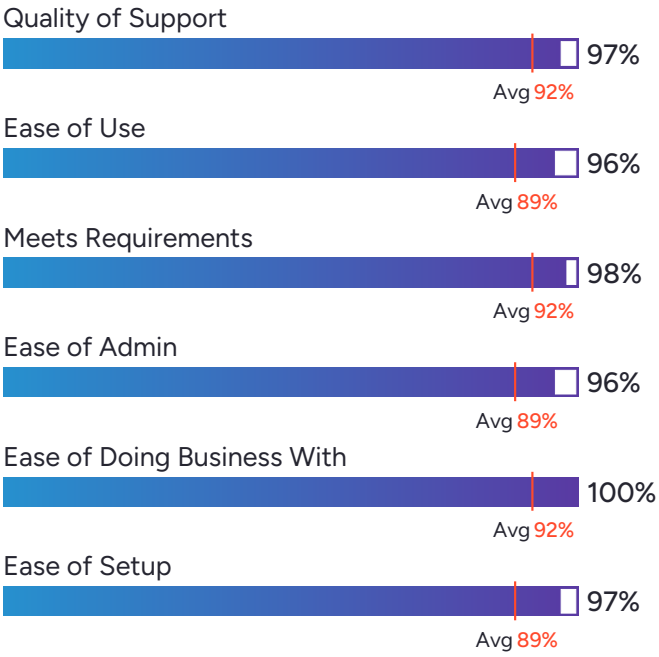
Torq

4.8 ★★★★★ (151)

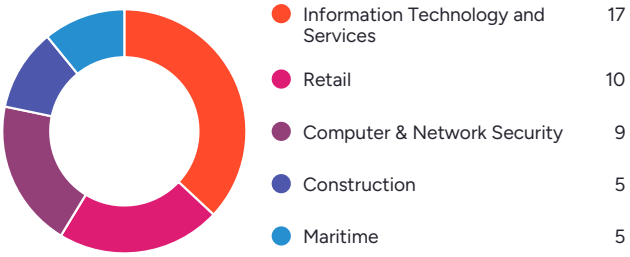
Leader

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 98%. 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.

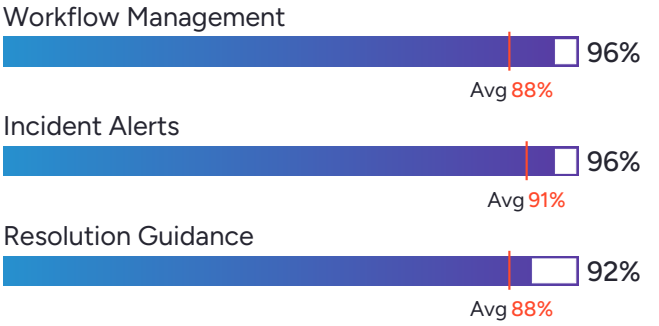
Satisfaction Ratings



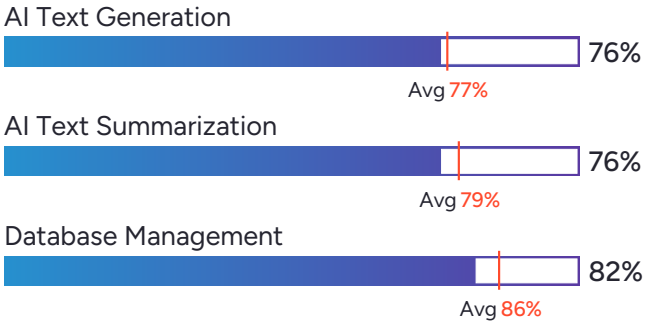
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
torq

HQ Location
New York, US

Year Founded
2020

Employees (Listed On Linkedin)
393

Company Website
torq.io

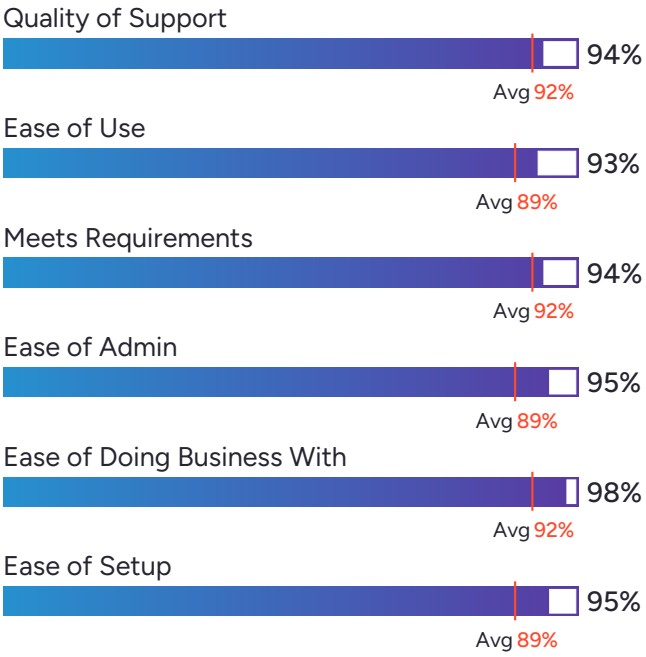
Cynet

4.7 ★★★★½ (247)

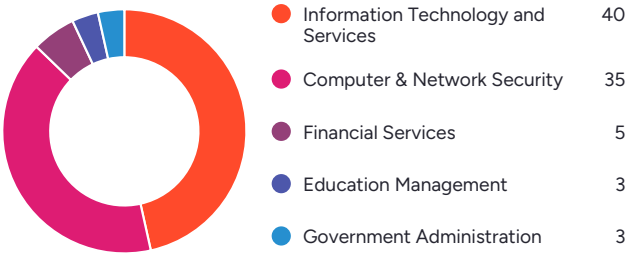
SPRING 2026 Leader

Cynet 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, 97% of users believe it is headed in the right direction, and users said they would be likely to recommend Cynet at a rate of 96%. Cynet 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.

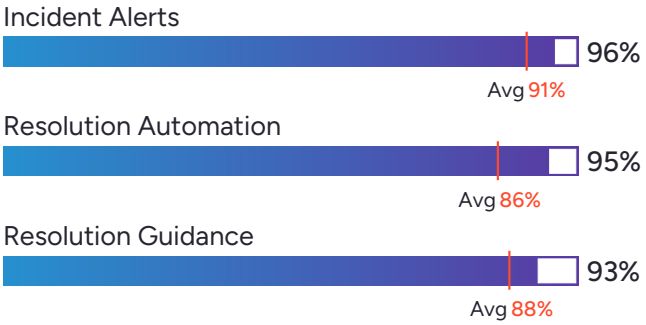
Satisfaction Ratings



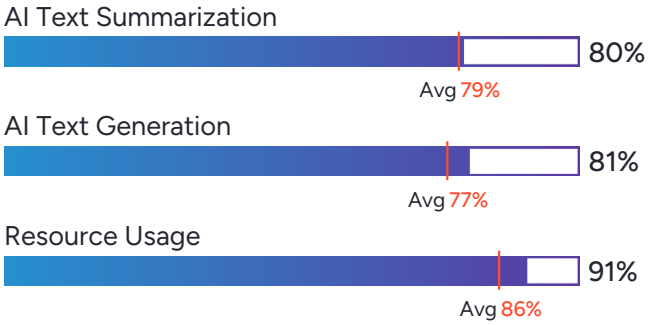
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Cynet

HQ Location
Boston, MA

Year Founded
2014

Employees (Listed On Linkedin)
329

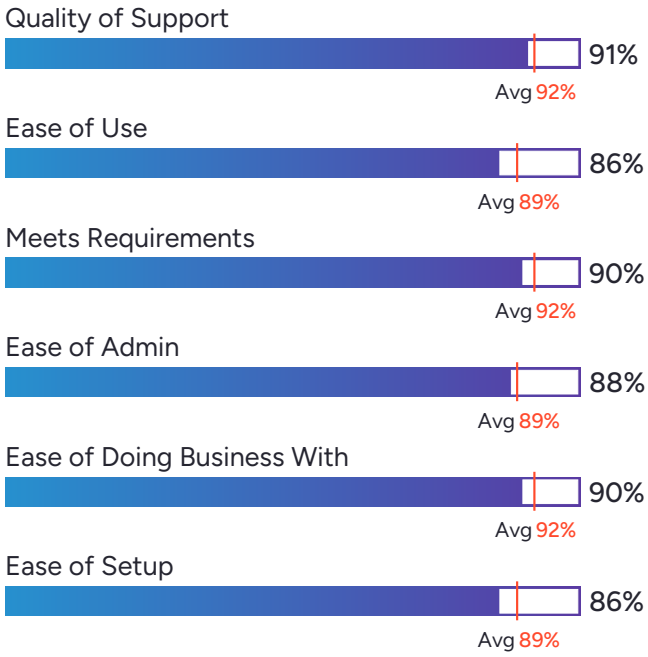
Company Website
www.cynet.com

Dynatrace

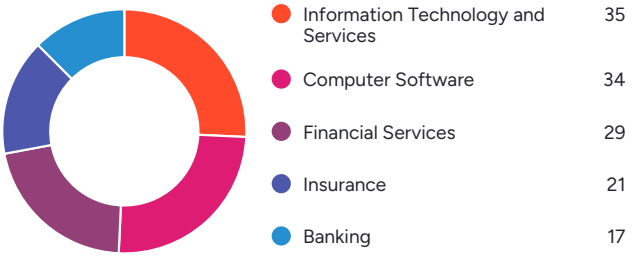
4.5 ★★★★½ (1,359)

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, 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.

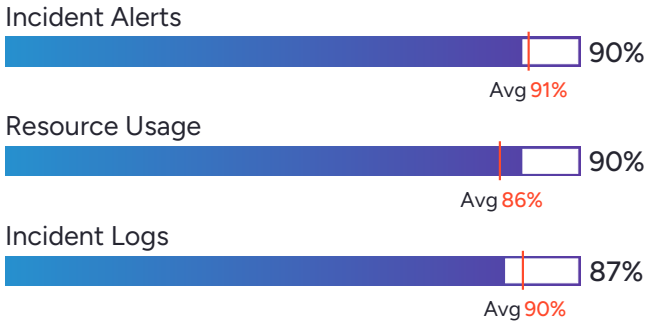
Satisfaction Ratings



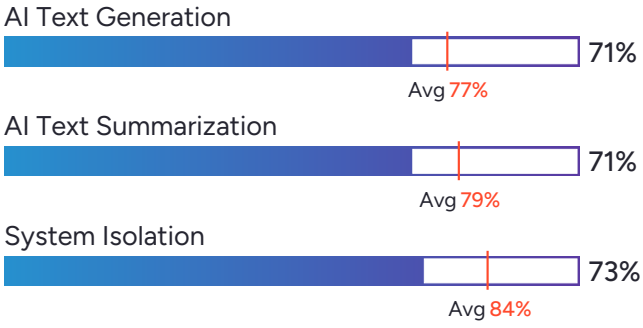
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Dynatrace

HQ Location
Boston, MA

Year Founded
2005

Employees (Listed On Linkedin)
5,800

Company Website
dynatrace.com

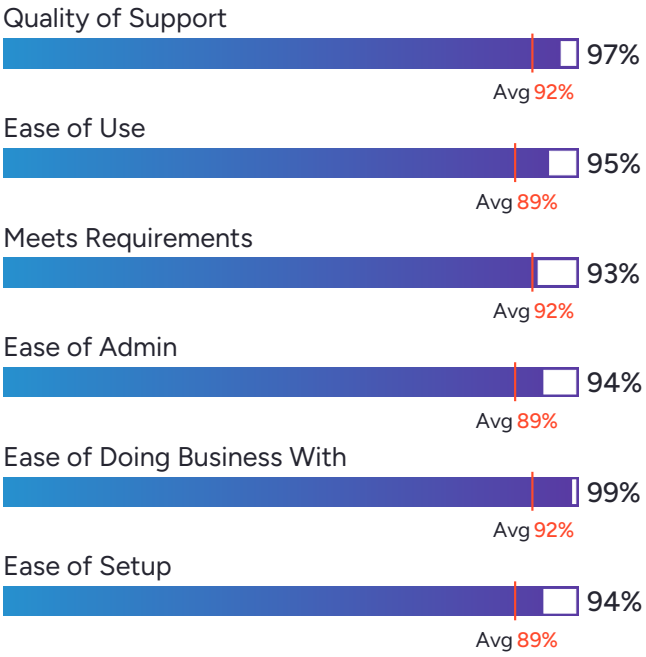
Tines

4.8 ★★★★★ (257)

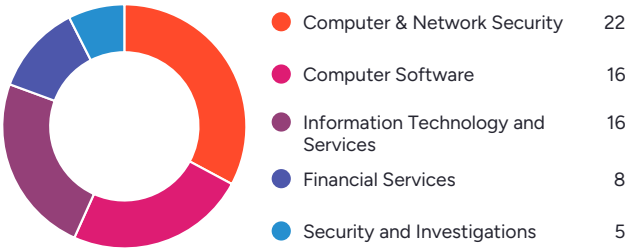
Leader

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, 97% 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.

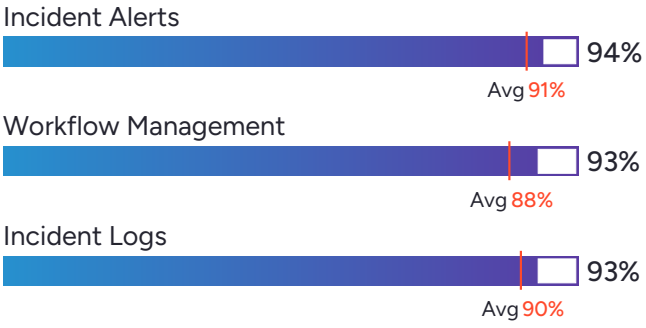
Satisfaction Ratings



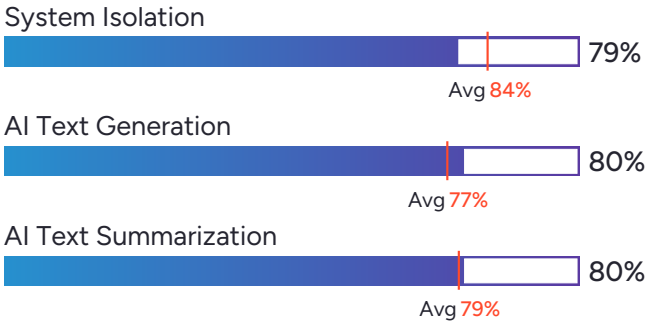
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Tines

HQ Location
Dublin, IE

Year Founded
2018

Employees (Listed On Linkedin)
538

Company Website
www.tines.com

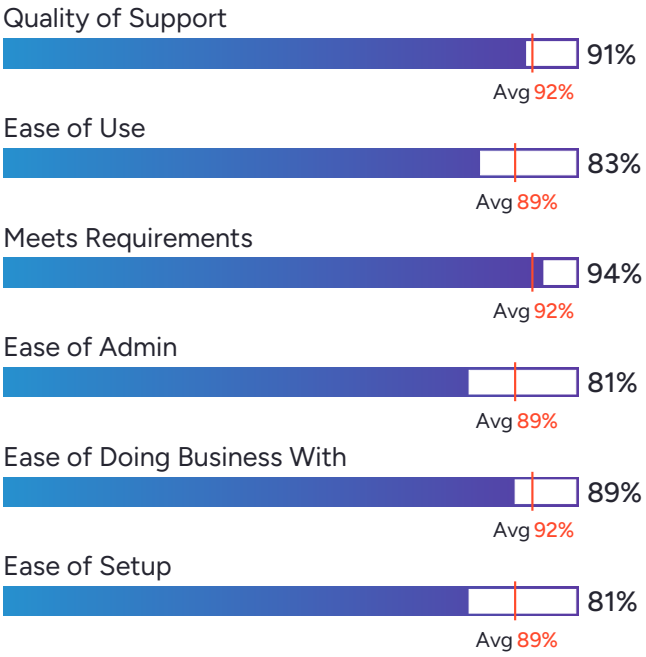
ServiceNow Security Operations

4.4 ★★★★½ (36)

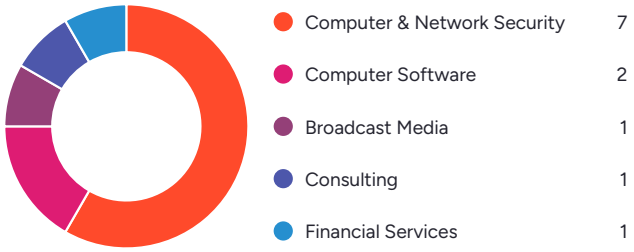
SPRING 2026 Leader

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 87%. ServiceNow Security Operations is also in the Risk-Based Vulnerability Management, Security Orchestration, Automation, and Response (SOAR), and Threat Intelligence categories.

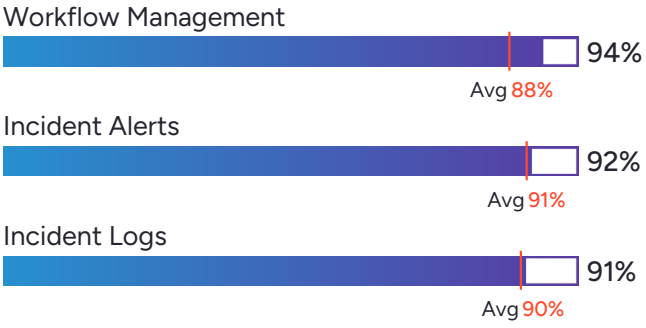
Satisfaction Ratings



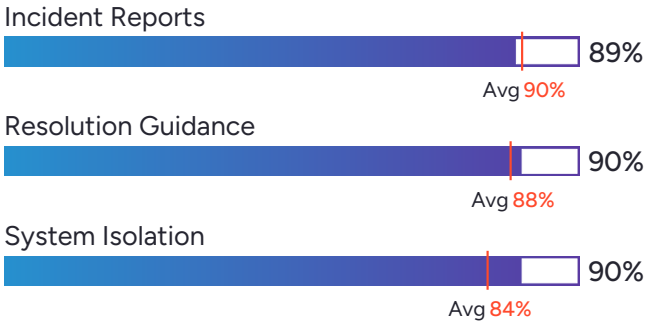
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
ServiceNow

HQ Location
Santa Clara, CA

Year Founded
2004

Employees (Listed On Linkedin)
31,344

Company Website
servicenow.com

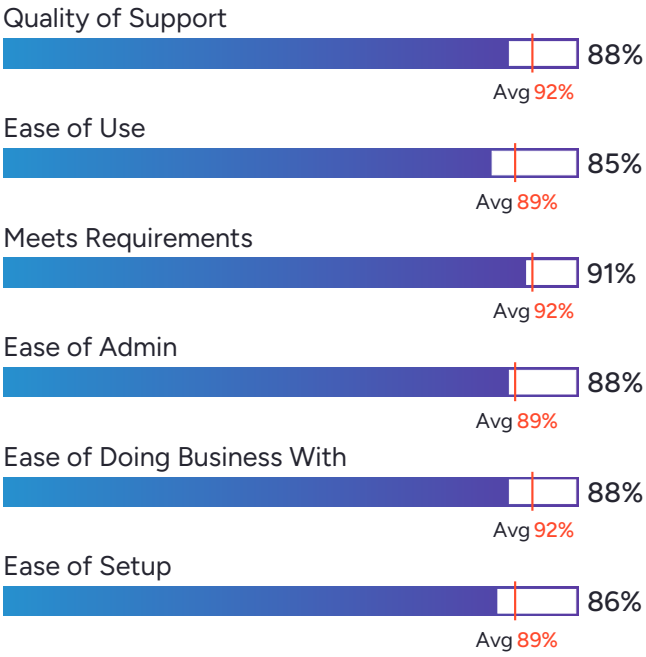
Sumo Logic

4.4 (382)

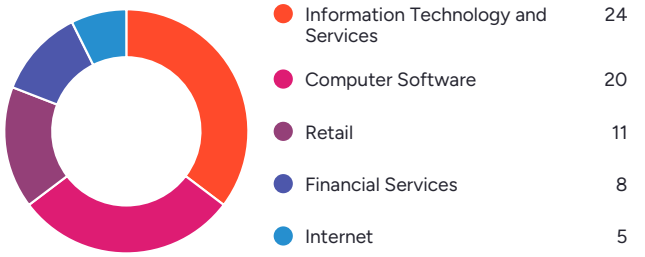
Leader

Sumo Logic 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, 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 Observability Software, AI Agents For Business Operations, Cloud Security Monitoring and Analytics, Security Orchestration, Automation, and Response (SOAR), Log Monitoring, Cloud Infrastructure Monitoring, Container Monitoring, Log Analysis, Security Information and Event Management (SIEM), and Application Performance Monitoring (APM) categories.

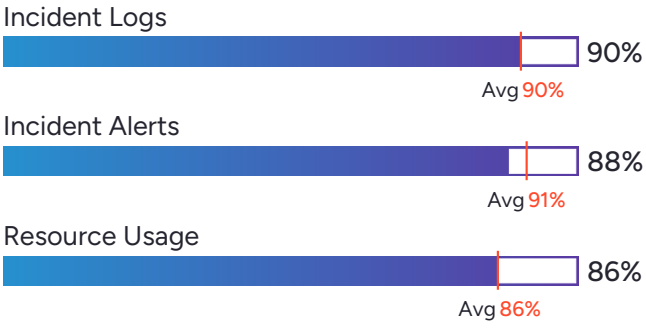
Satisfaction Ratings



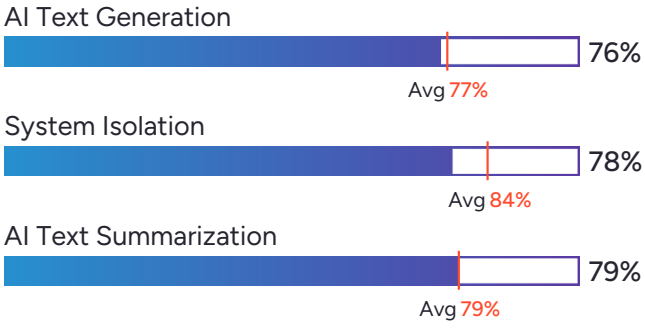
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Sumo Logic

HQ Location
Redwood City, CA

Year Founded
2010

Employees (Listed On Linkedin)
808

Company Website
sumologic.com

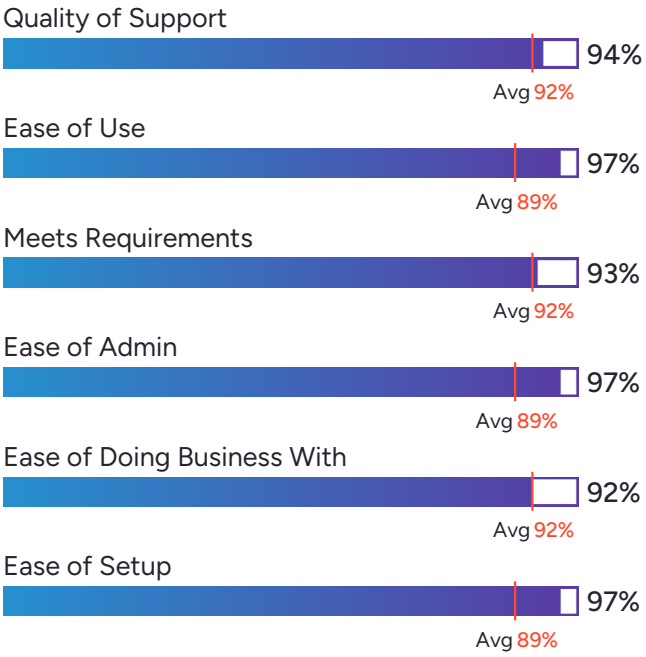
Barracuda Incident Response

4.5 ★★★★½ (16)

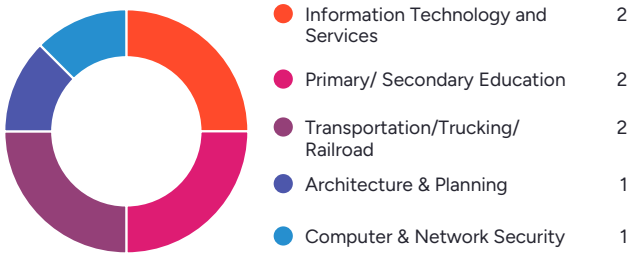
SPRING 2026 High Performer

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. 93% 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 Barracuda Incident Response at a rate of 91%. Barracuda Incident Response is also in the Security Orchestration, Automation, and Response (SOAR) category.

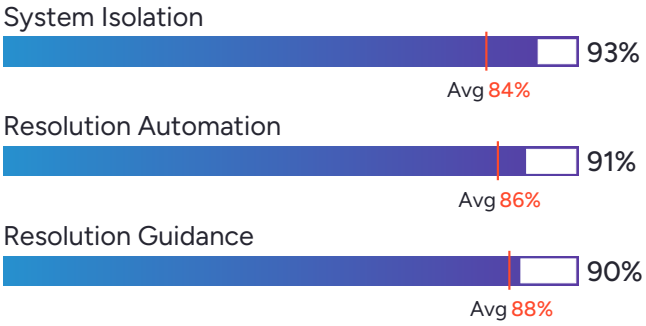
Satisfaction Ratings



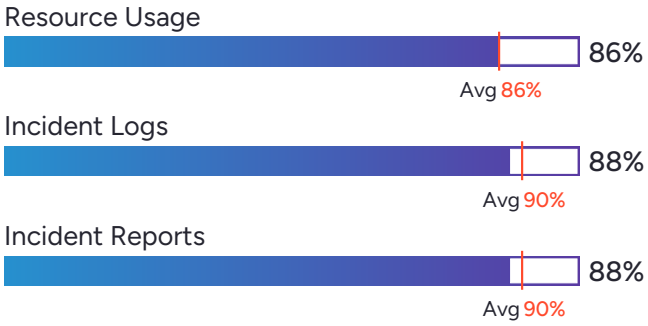
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Barracuda

HQ Location
Campbell, CA

Year Founded
2002

Employees (Listed On Linkedin)
2,229

Company Website
barracuda.com

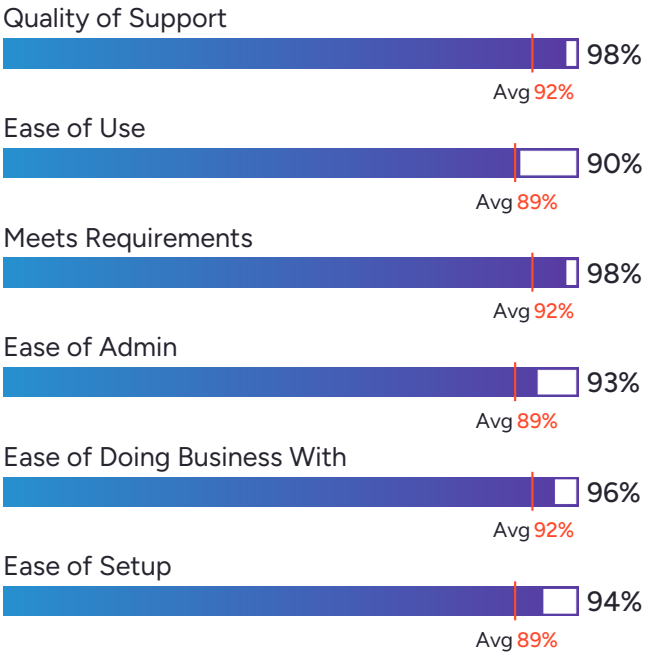
SpinOne

4.8 ★★★★★ (121)

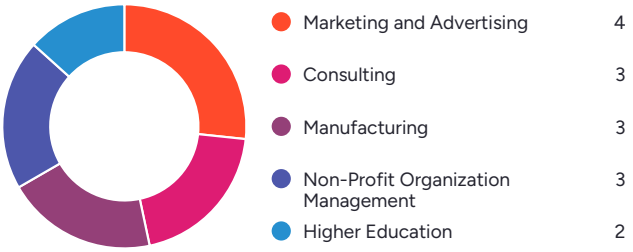
SPRING 2026 High Performer

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), SaaS Backup, and Data Security Posture Management (DSPM) categories.

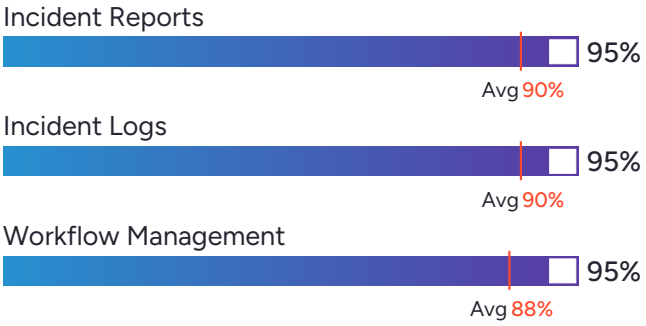
Satisfaction Ratings



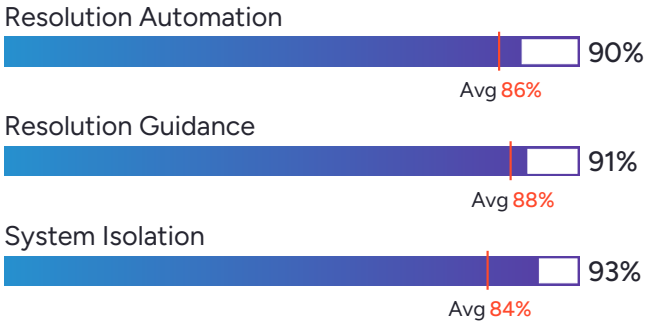
Top Industries Represented



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

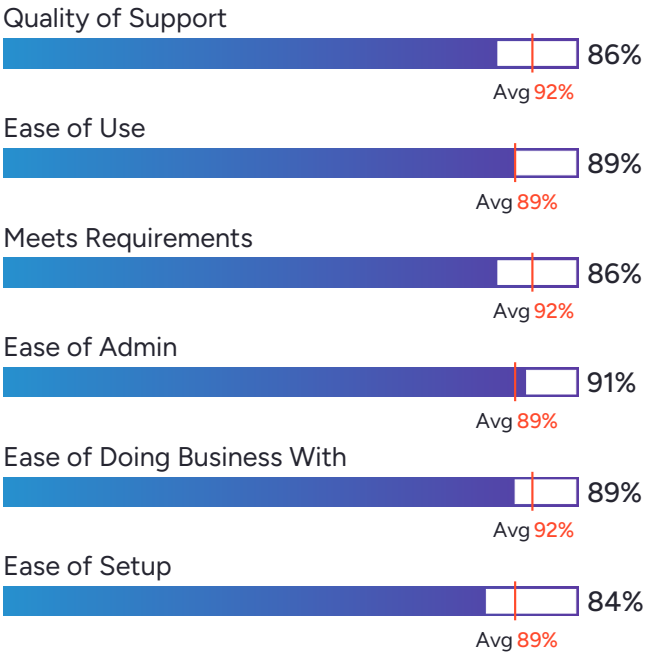
CYREBRO

4.3 ★★★★½ (130)

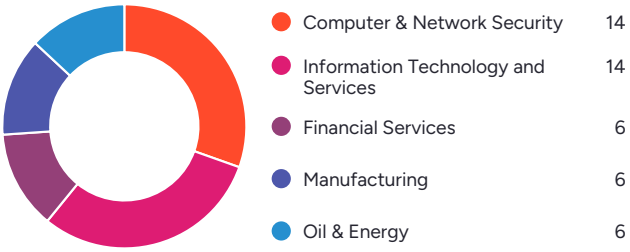
SPRING 2026 High Performer

CYREBRO 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. 90% 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 CYREBRO at a rate of 87%. CYREBRO is also in the Managed Detection and Response (MDR) and Threat Intelligence categories.

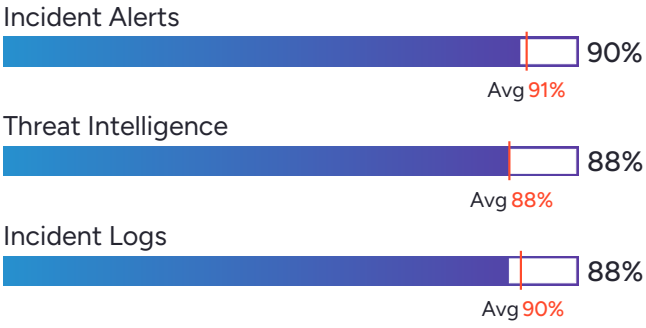
Satisfaction Ratings



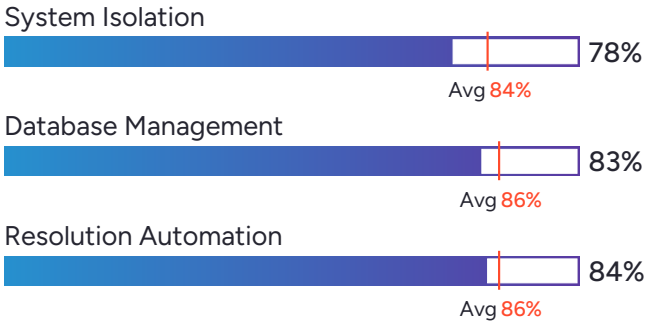
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
CYREBRO

HQ Location
Tel Aviv, IL

Year Founded
2013

Employees (Listed On Linkedin)
99

Company Website
www.cyrebro.io

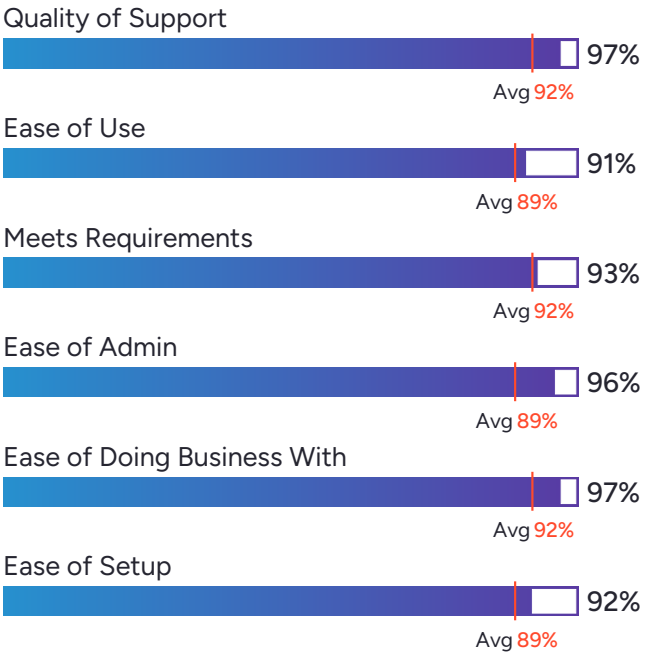
OneTrust Tech Risk & Compliance

4.6 ★★★★½ (109)

SPRING 2026 High Performer

OneTrust Tech Risk & Compliance 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 OneTrust Tech Risk & Compliance at a rate of 93%. 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)
2,543

Company Website
onetrust.com

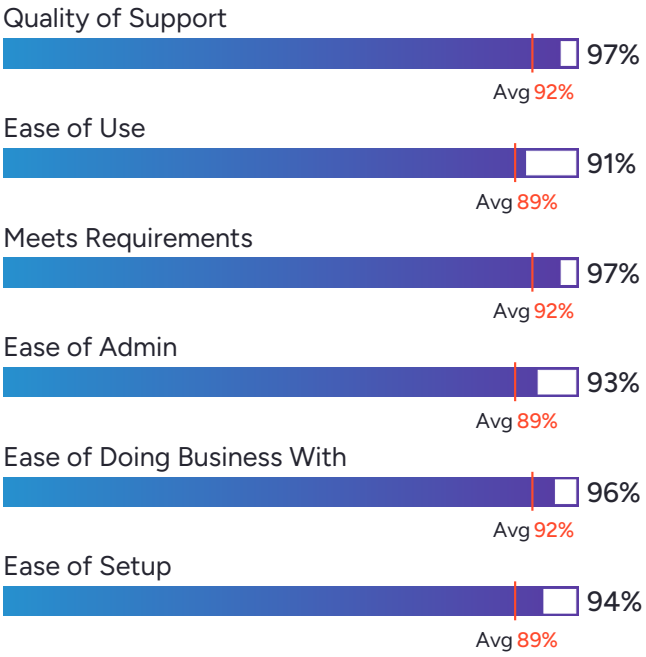
Pondurance

4.7 ★★★★½ (13)

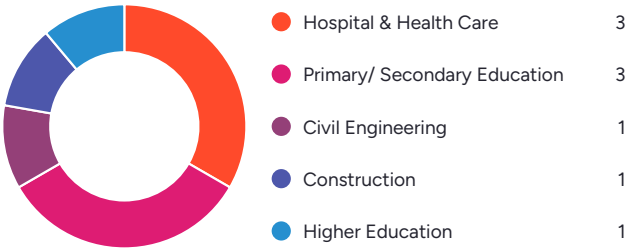
SPRING 2026 High Performer

Pondurance 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 Pondurance at a rate of 94%. Pondurance is also in the Managed Detection and Response (MDR) category.

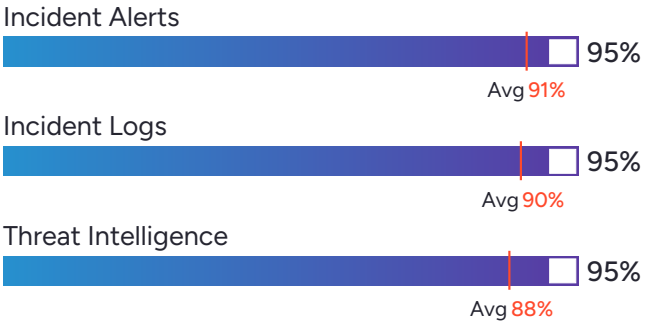
Satisfaction Ratings



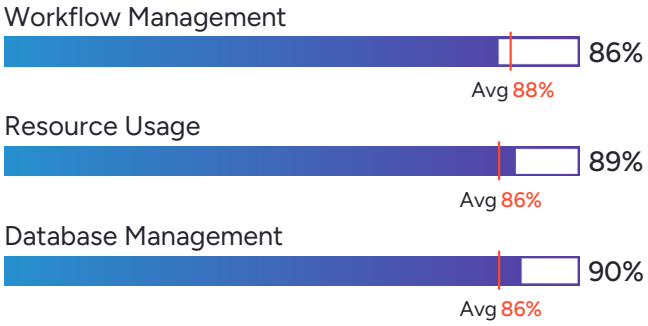
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Pondurance

HQ Location
Indianapolis, US

Year Founded
2008

Employees (Listed On Linkedin)
119

Company Website
pondurance.com

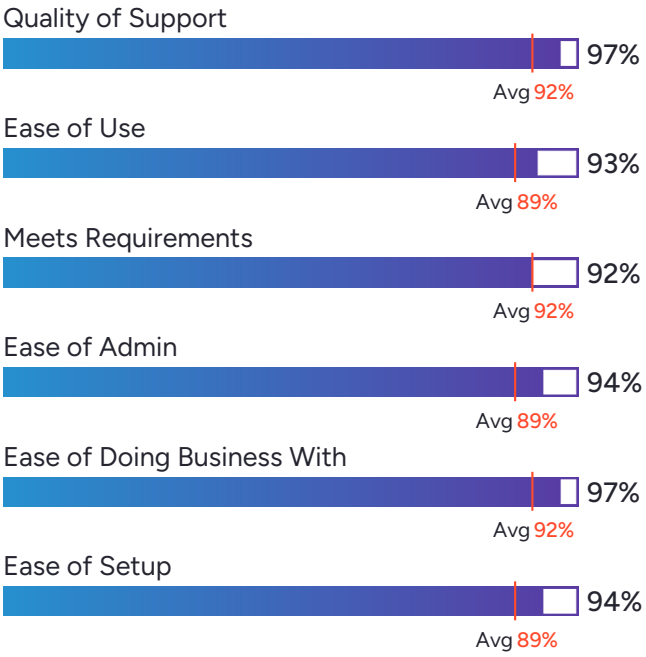
Blumira Automated Detection & Response

4.6 ★★★★½ (123)

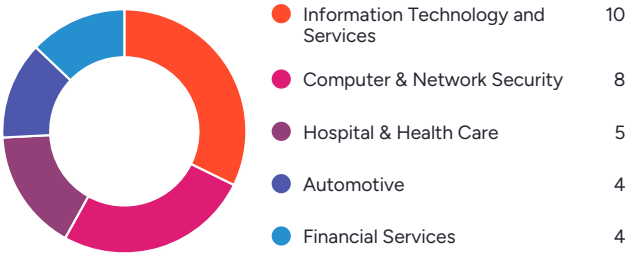
SPRING 2026 High Performer

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 94%. 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.

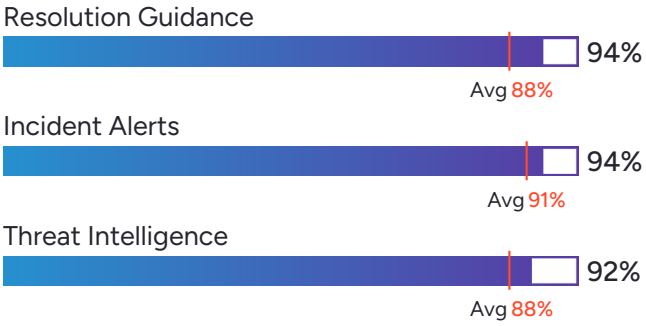
Satisfaction Ratings



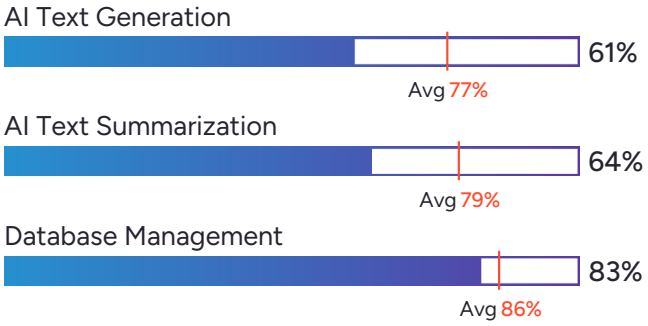
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Blumira

HQ Location
Ann Arbor, Michigan

Year Founded
2018

Employees (Listed On Linkedin)
67

Company Website
blumira.com

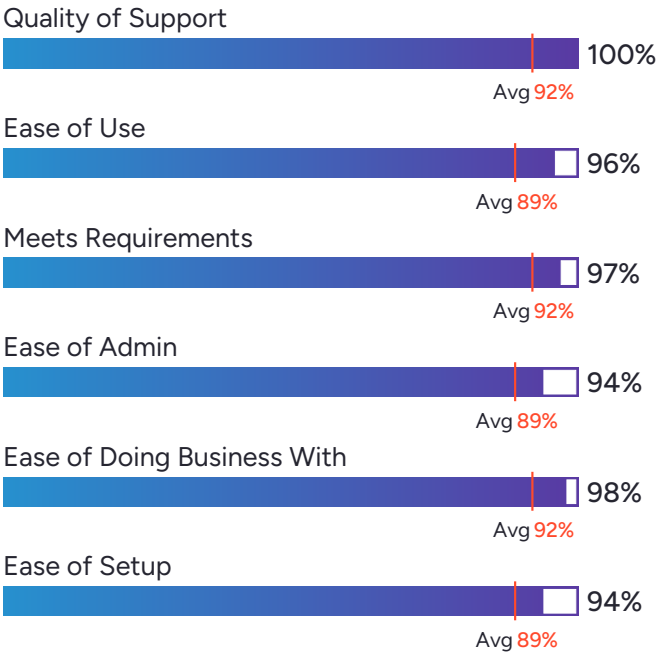
UnderDefense MAXI

4.8 ★★★★★ (26)

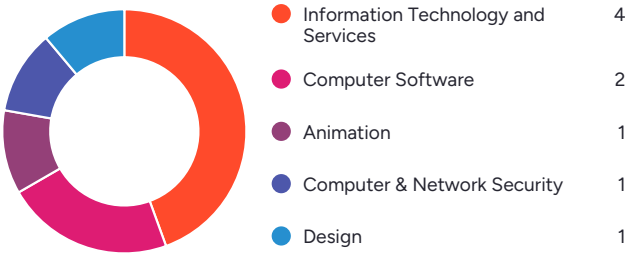
SPRING 2026 High Performer

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.

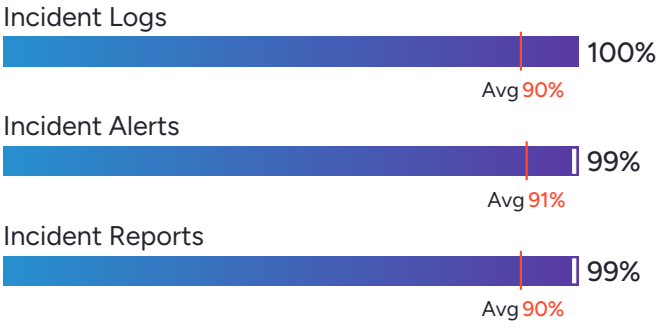
Satisfaction Ratings



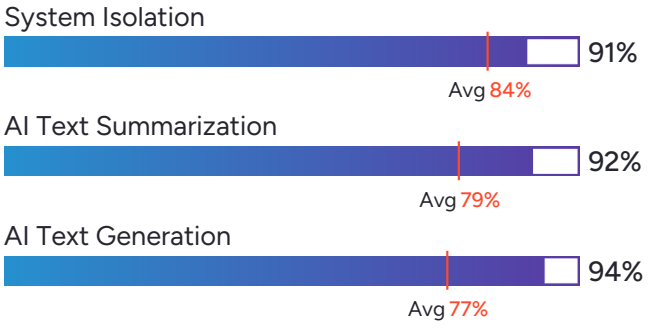
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
UnderDefense

HQ Location
New York, NY

Year Founded
2017

Employees (Listed On Linkedin)
134

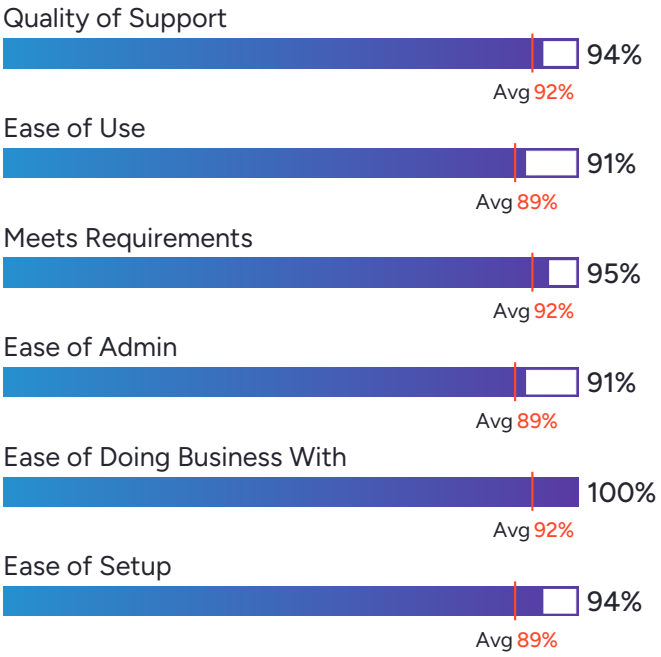
Company Website
underdefense.com

Splunk On-Call

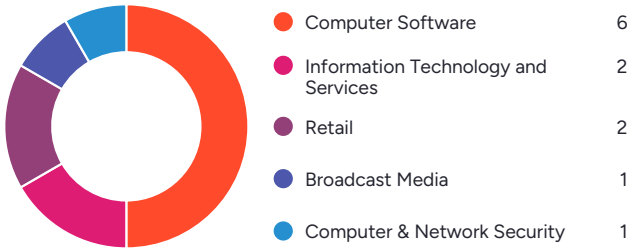
4.5 ★★★★½ (51)

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)
95,386

Company Website
www.cisco.com

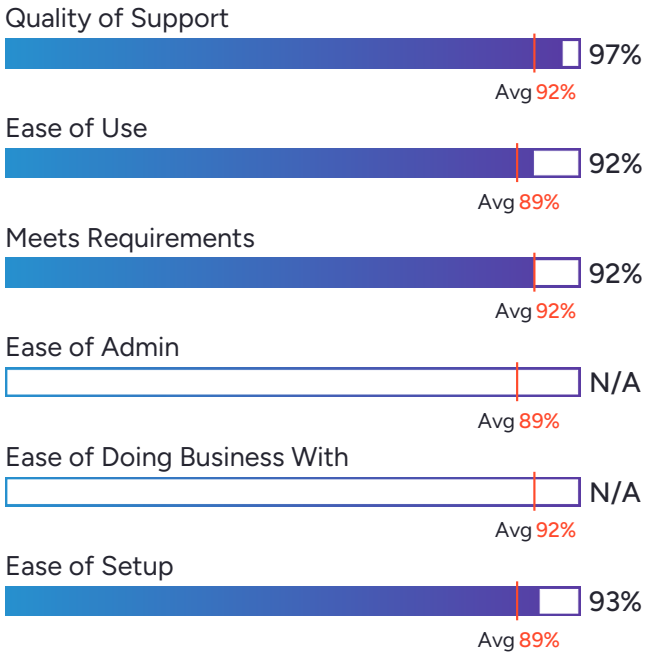
Belkasoft

4.7 ★★★★½ (132)

SPRING 2026 High Performer

Belkasoft 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 Belkasoft at a rate of 90%. Belkasoft is also in the Digital Forensics category.

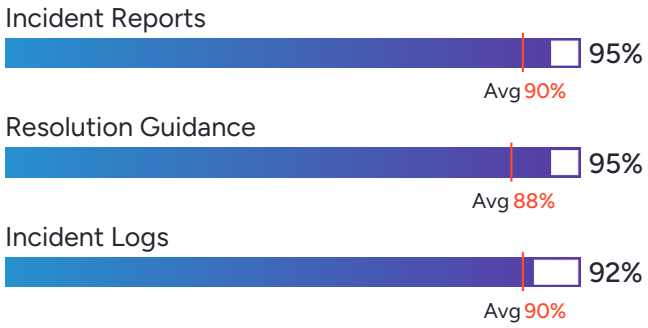
Satisfaction Ratings



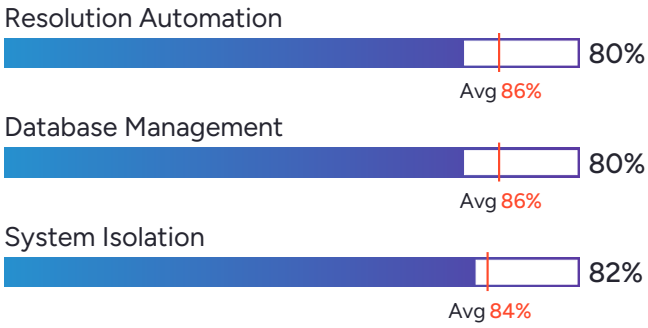
*N/A is displayed when fewer than five responses were received for the question.

Top Industries Represented

Highest-Rated Features



Lowest-Rated Features



Ownership
Belkasoft

HQ Location
Sunnyvale, California

Year Founded
2002

Employees (Listed On Linkedin)
35

Company Website
belkasoft.com

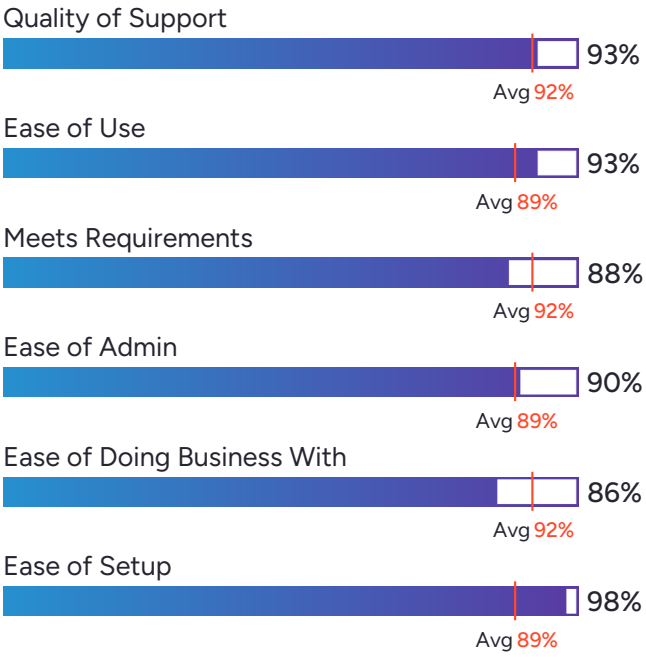
Intezer

4.5 ★★★★½ (193)

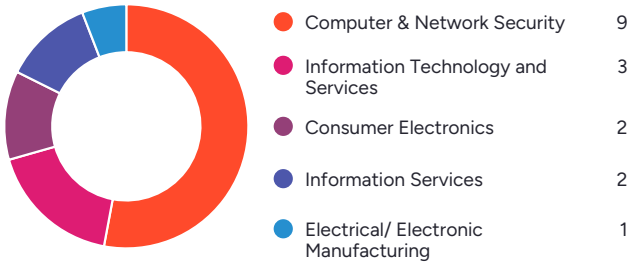
High Performer

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, 93% 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, AI SOC Agents, Managed Detection and Response (MDR), Threat Intelligence, Security Orchestration, Automation, and Response (SOAR), Endpoint Detection & Response (EDR), and Network Sandboxing categories.

Satisfaction Ratings



Top Industries Represented



Ownership
Intezer

HQ Location
New York

Year Founded
2015

Employees (Listed On Linkedin)
82

Company Website
intezer.com

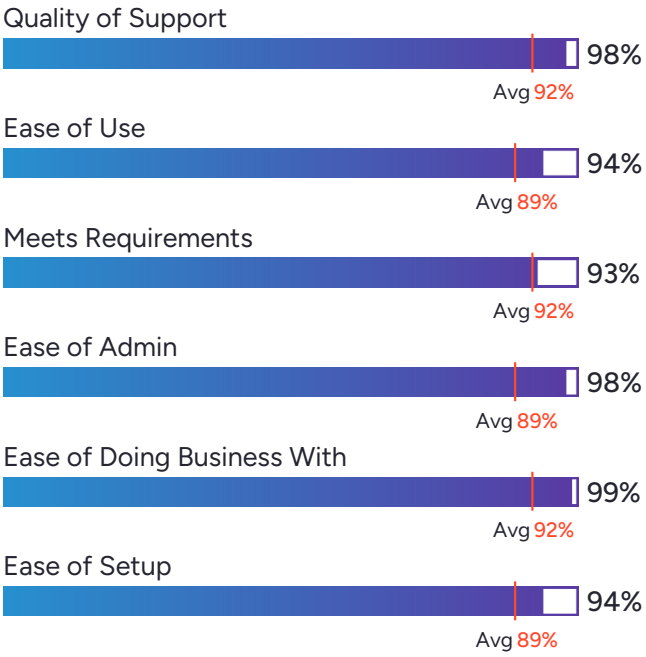
Defendify All-In-One Cybersecurity Solution

4.7 ★★★★½ (57)

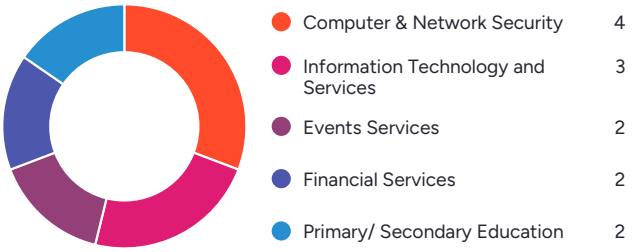
SPRING 2026 High Performer

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, and Threat Intelligence categories.

Satisfaction Ratings

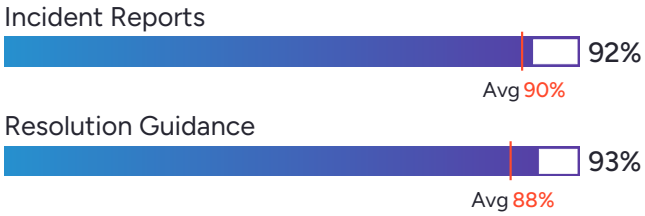


Top Industries Represented



Highest-Rated Features

Lowest-Rated Features



Ownership
Defendify

HQ Location
Portland, Maine

Year Founded
2017

Employees (Listed On Linkedin)
40

Company Website
defendify.com

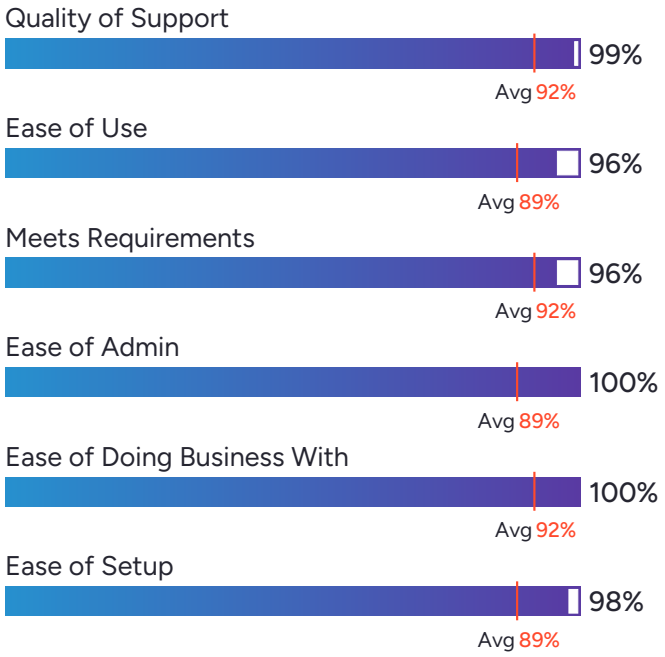
SIRP

4.7 ★★★★½ (27)

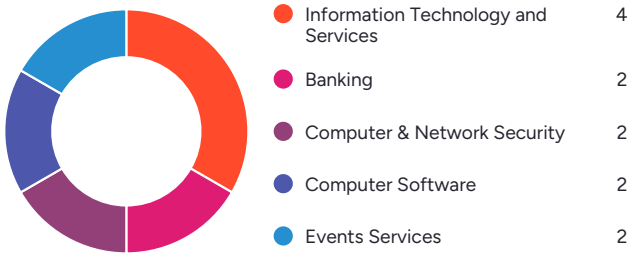
SPRING 2026 High Performer

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, AI SOC Agents, and Security Orchestration, Automation, and Response (SOAR) categories.

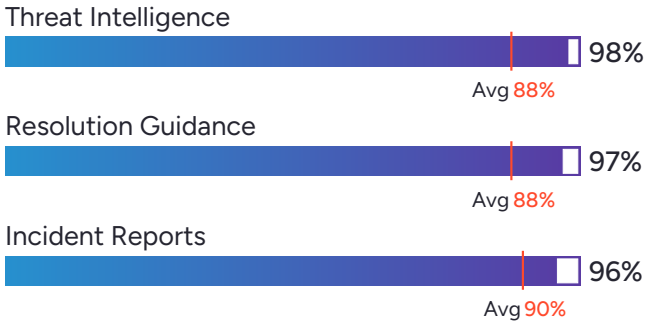
Satisfaction Ratings



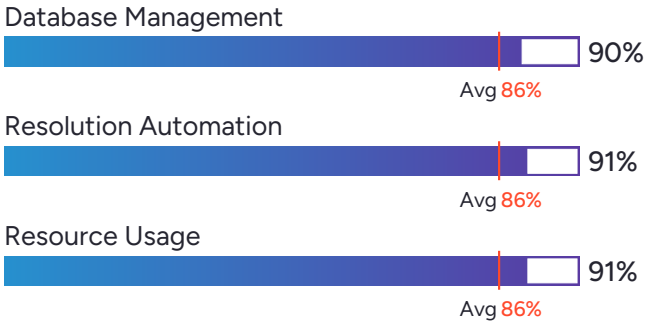
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
SIRP

HQ Location
Bethesda, Maryland

Year Founded
2017

Employees (Listed On Linkedin)
59

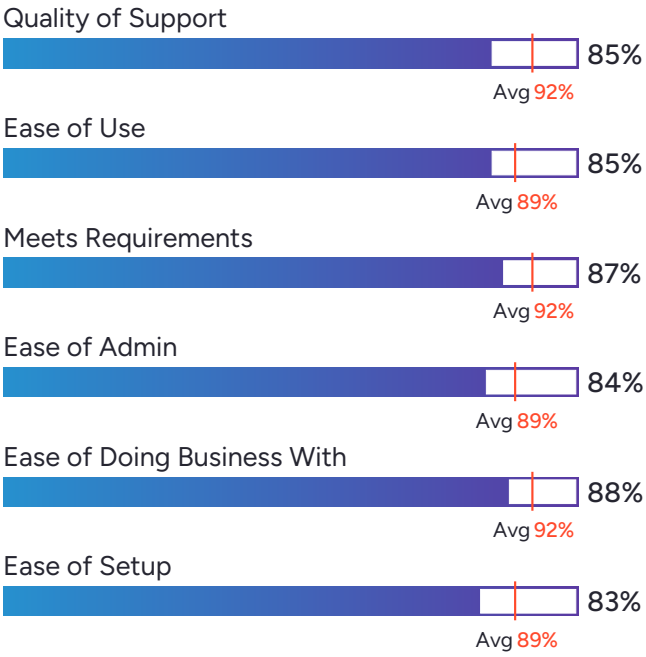
Company Website
www.sirp.io

Palo Alto Cortex XSIAM

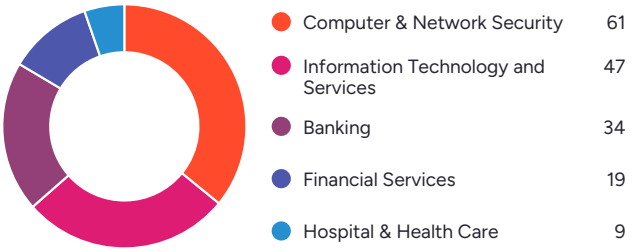
4.3 ★★★★½ (474)

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.

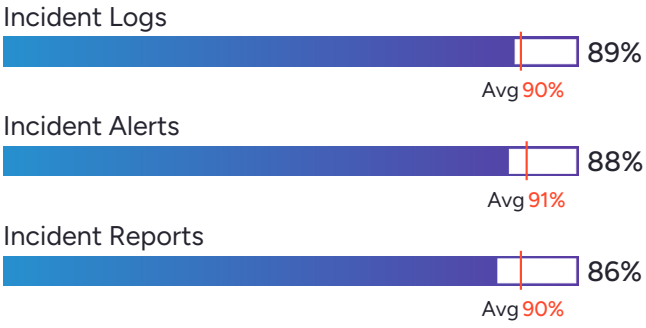
Satisfaction Ratings



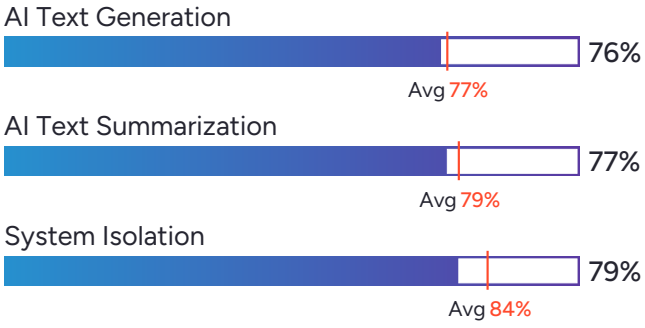
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Palo Alto Networks

HQ Location
Santa Clara, CA

Year Founded
2005

Employees (Listed On Linkedin)
18,396

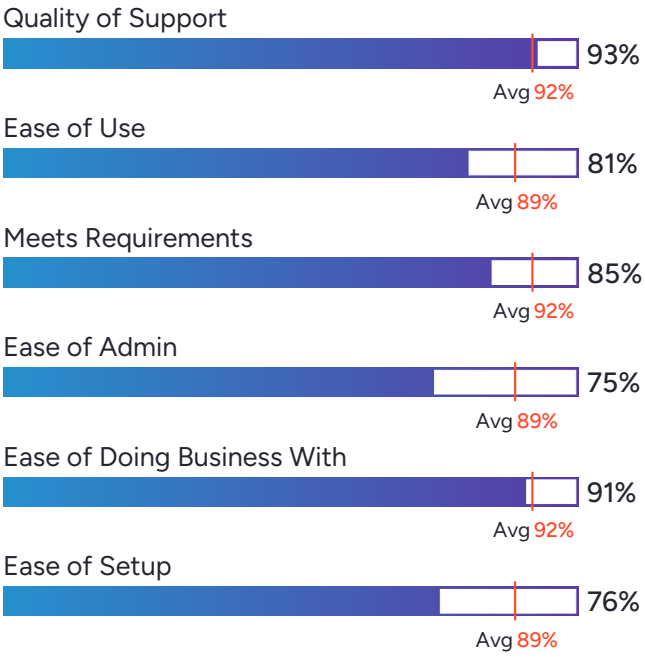
Company Website
paloaltonetworks.com

Resolver

4.3 ★★★★½ (180)

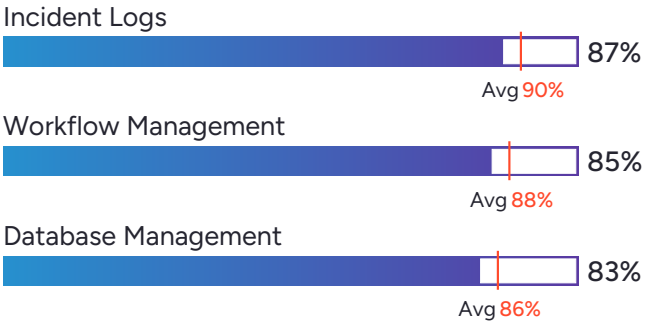
Resolver has been named a Contender product based on having a relatively low customer Satisfaction score and large Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 96% of users rated it 4 or 5 stars, 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, and Physical Security categories.

Satisfaction Ratings

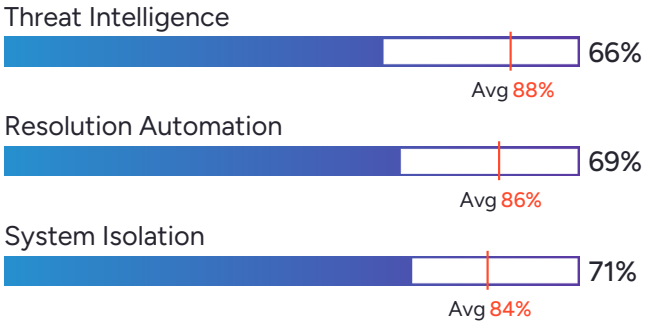


Top Industries Represented

Highest-Rated Features



Lowest-Rated Features



Ownership
Resolver

HQ Location
Toronto, Canada

Employees (Listed On Linkedin)
727

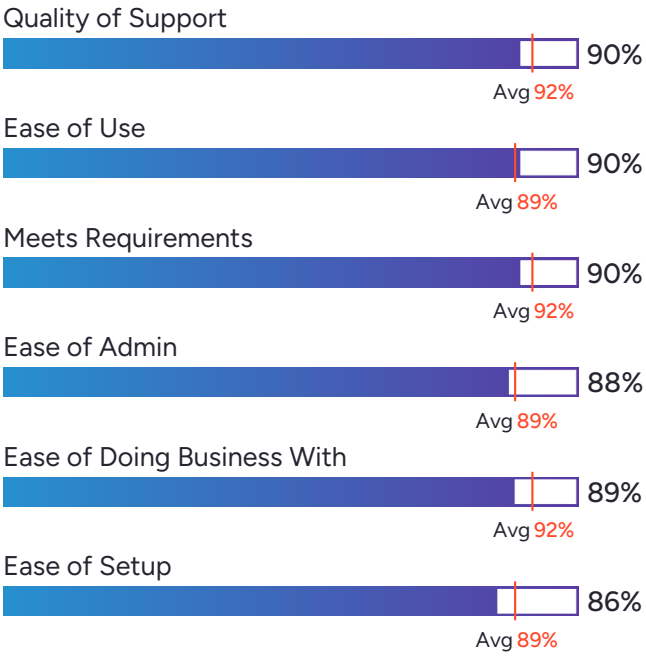
Company Website
resolver.com

InsightIDR

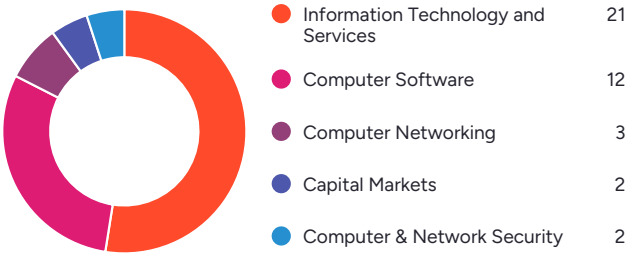
4.4 ★★★★½ (73)

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, 90% of users believe it is headed in the right direction, and users said they would be likely to recommend InsightIDR at a rate of 89%. 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

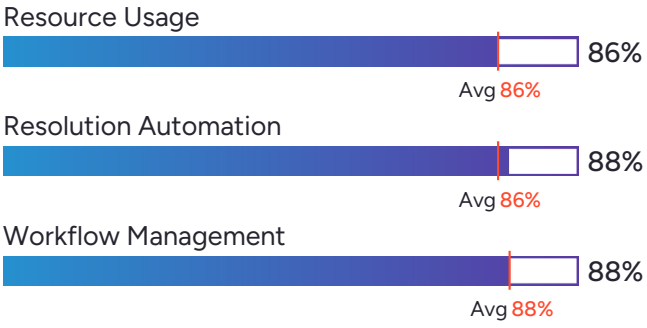


Top Industries Represented



Highest-Rated Features

Lowest-Rated Features



Ownership
Rapid7

HQ Location
Boston, MA

Year Founded
2000

Employees (Listed On Linkedin)
3,249

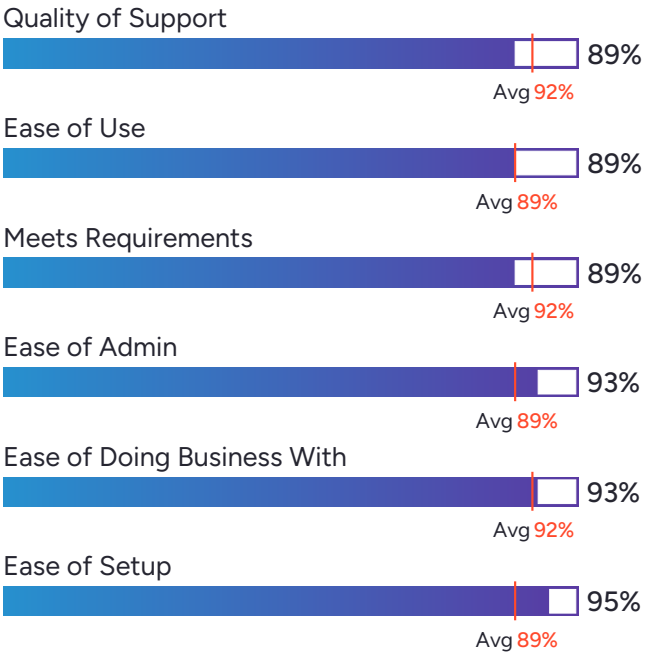
Company Website
www.rapid7.com

Proofpoint Threat Response

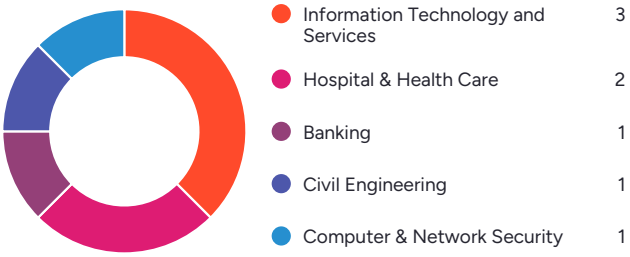
4.6 ★★★★½ (17)

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.

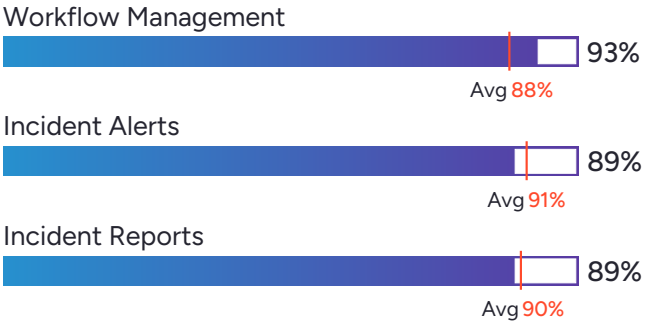
Satisfaction Ratings



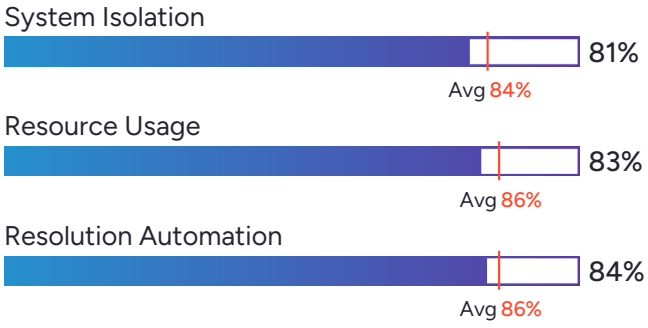
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Proofpoint

HQ Location
Sunnyvale, CA

Year Founded
2002

Employees (Listed On Linkedin)
5,020

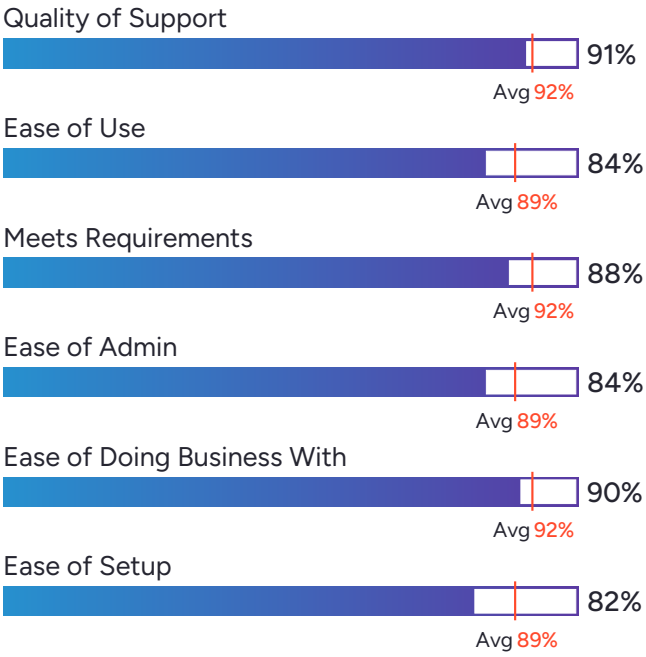
Company Website
proofpoint.com

Splunk SOAR (Security Orchestration, Automation and Response)

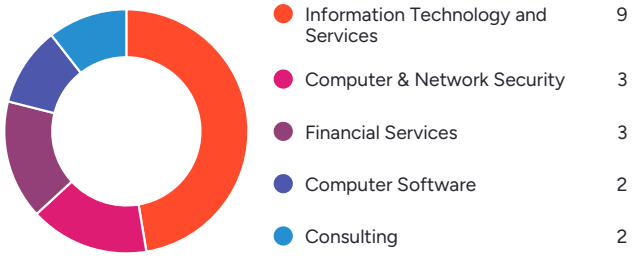
4.4 ★★★★½ (40)

Splunk SOAR (Security Orchestration, Automation and Response) 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. 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.

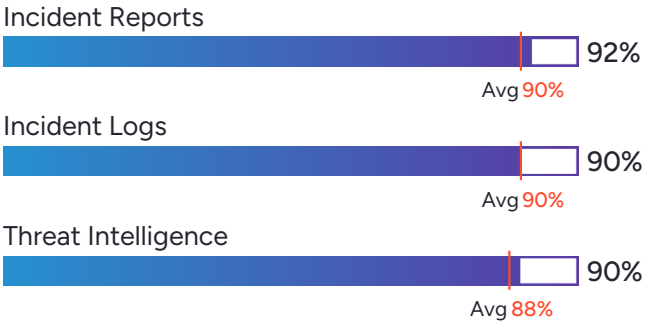
Satisfaction Ratings



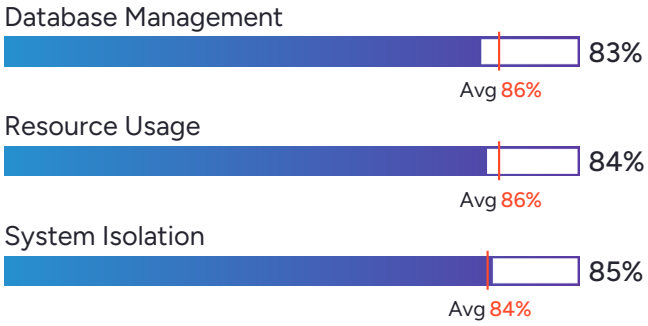
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Cisco

HQ Location
San Jose, CA

Year Founded
1984

Employees (Listed On Linkedin)
95,386

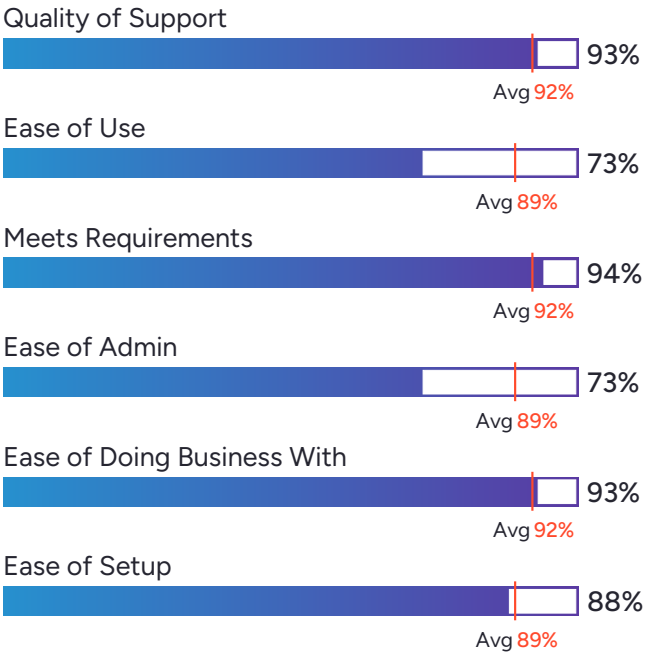
Company Website
www.cisco.com

Darktrace / NETWORK

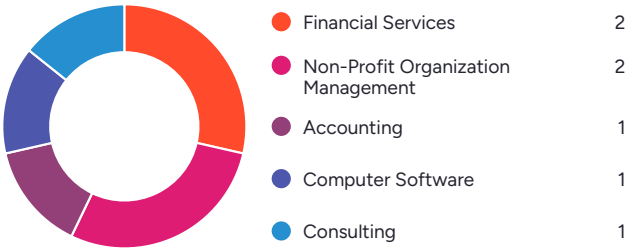
4.4 ★★★★½ (45)

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 Cloud Detection and Response (CDR), Network Detection and Response (NDR), Cloud Security Monitoring and Analytics, Network Traffic Analysis (NTA), Managed Detection and Response (MDR), Intrusion Detection and Prevention Systems (IDPS), Cloud Workload Protection Platforms, Network Monitoring, and Extended Detection and Response (XDR) Platforms categories.

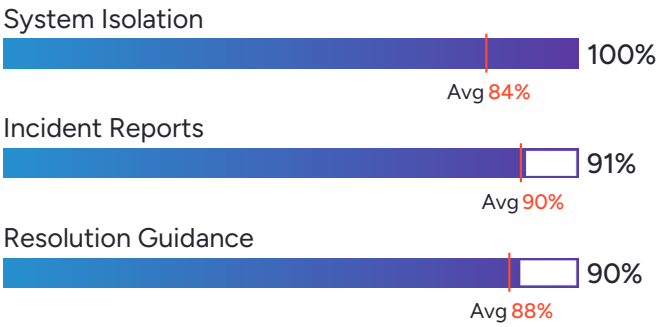
Satisfaction Ratings



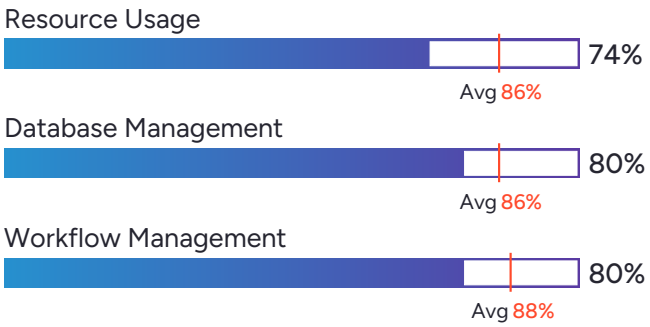
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Darktrace

HQ Location
Cambridgeshire, England

Year Founded
2013

Employees (Listed On Linkedin)
2,537

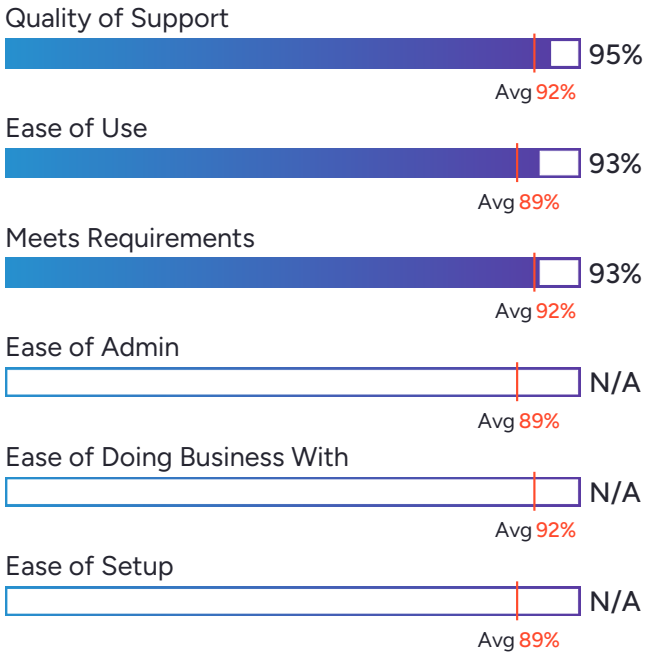
Company Website
darktrace.com

Splunk Synthetic Monitoring

4.5 ★★★★½ (25)

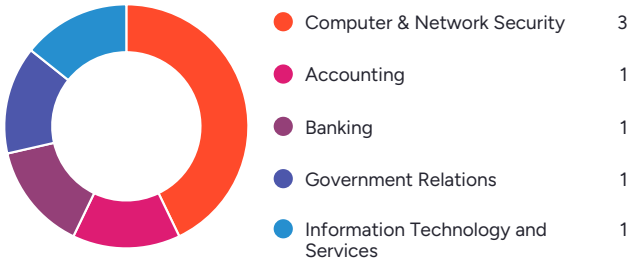
Splunk Synthetic Monitoring has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 4 or 5 stars,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

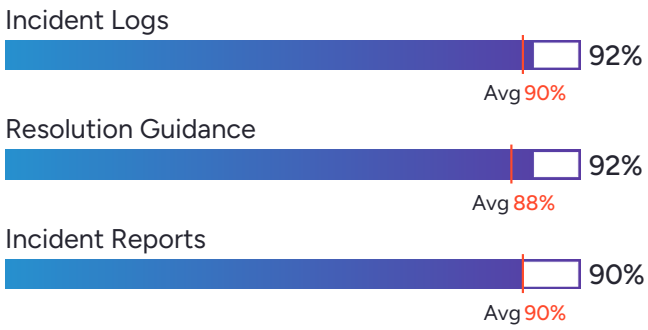


*N/A is displayed when fewer than five responses were received for the question.

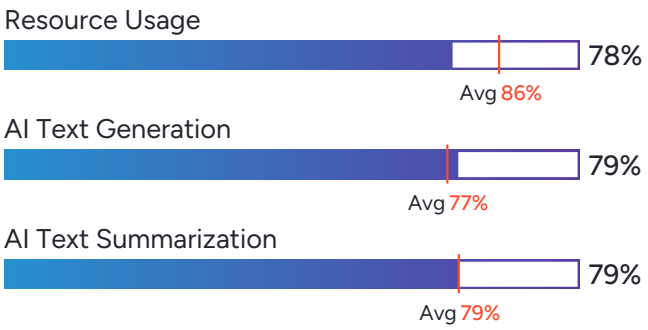
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Cisco

HQ Location
San Jose, CA

Year Founded
1984

Employees (Listed On Linkedin)
95,386

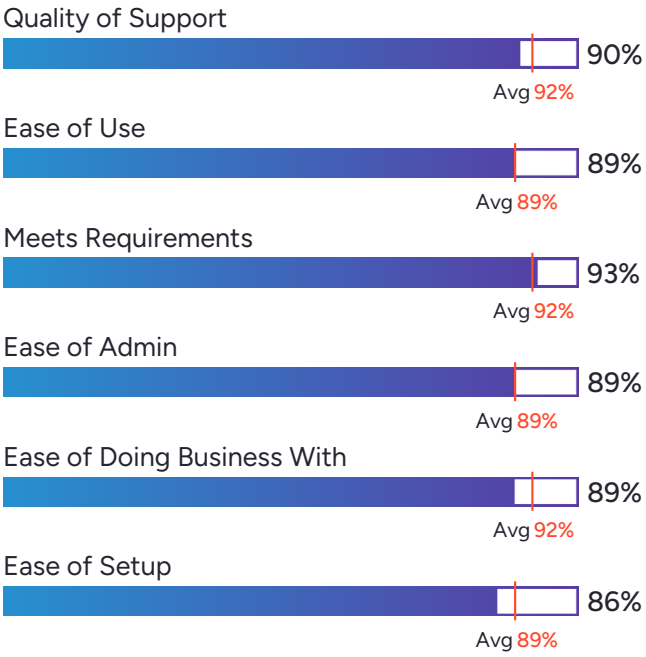
Company Website
www.cisco.com

Proofpoint Threat Response Auto-Pull

4.5 ★★★★½ (24)

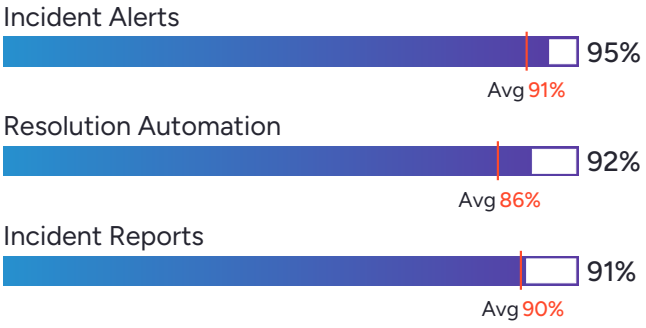
Proofpoint Threat Response Auto-Pull has been named a Contender product based on having a relatively low customer Satisfaction score and large Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 92% of users rated it 4 or 5 stars, 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

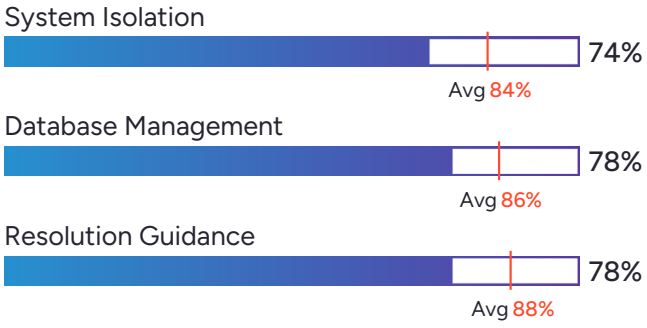


Top Industries Represented

Highest-Rated Features



Lowest-Rated Features



Ownership
Proofpoint

HQ Location
Sunnyvale, CA

Year Founded
2002

Employees (Listed On Linkedin)
5,020

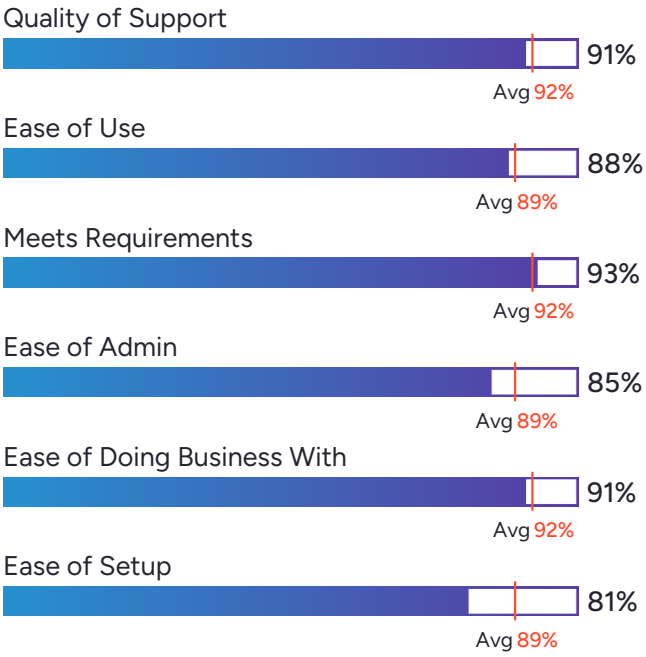
Company Website
proofpoint.com

LevelBlue USM Anywhere

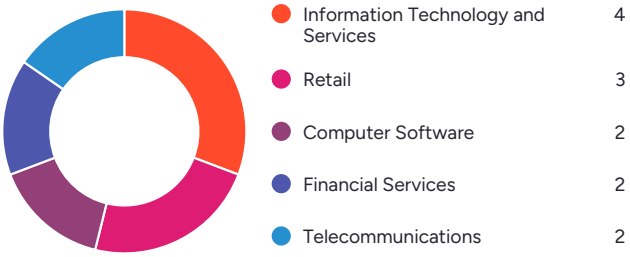
4.4 ★★★★½ (114)

LevelBlue USM Anywhere 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. 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 LevelBlue USM Anywhere at a rate of 91%. LevelBlue USM Anywhere is also in the Cloud Compliance, Intrusion Detection and Prevention Systems (IDPS), Vulnerability Scanner, and Security Information and Event Management (SIEM) categories.

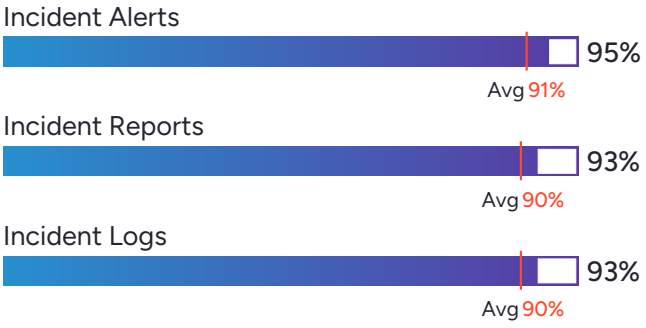
Satisfaction Ratings



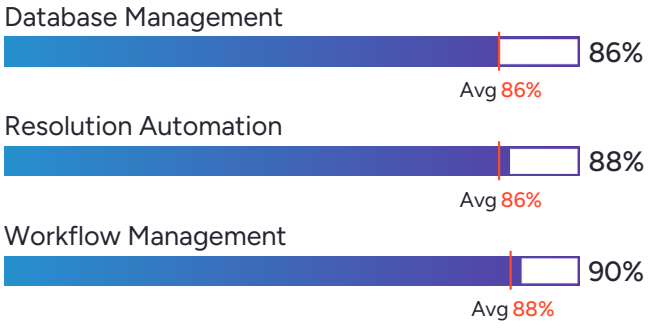
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
LevelBlue

HQ Location
Dallas, Texas, United States

Employees (Listed On Linkedin)
638

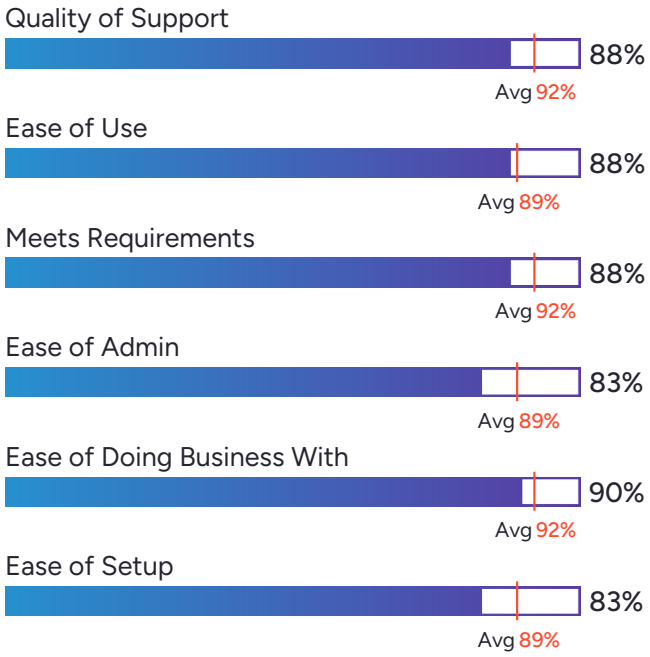
Company Website
levelblue.com

LogRhythm SIEM

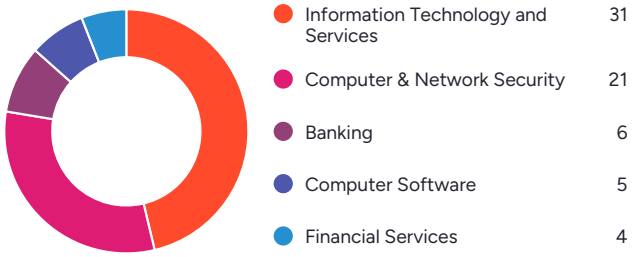
4.2 ★★★★☆ (152)

LogRhythm SIEM 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. 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.

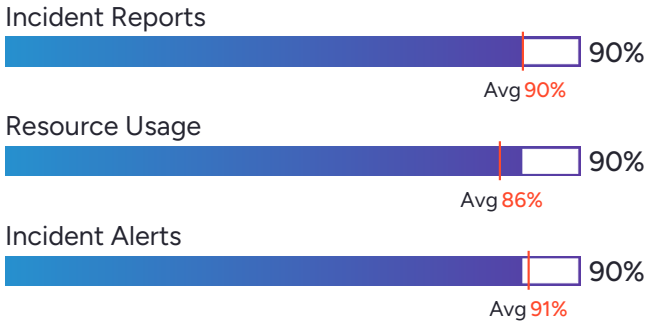
Satisfaction Ratings



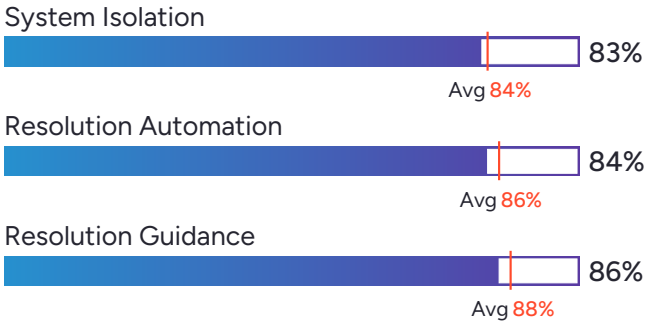
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Exabeam

HQ Location
Foster City, US

Year Founded
2013

Employees (Listed On Linkedin)
819

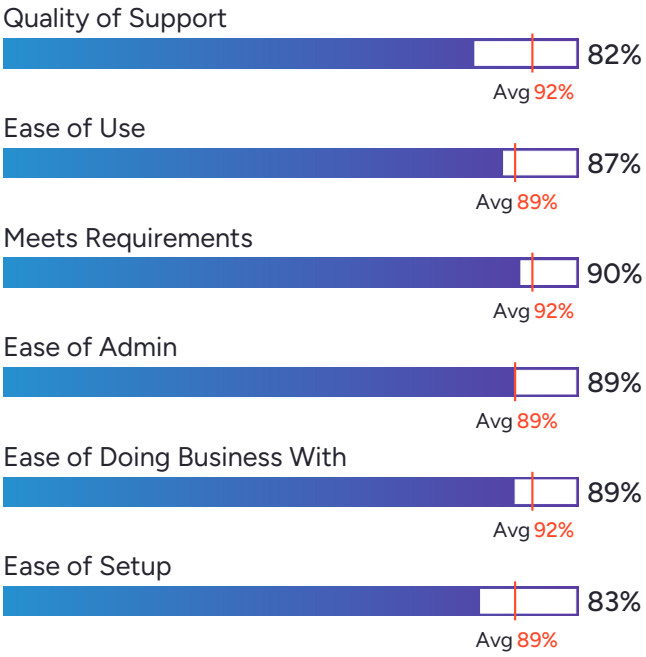
Company Website
exabeam.com

Wazuh - The Open Source Security Platform

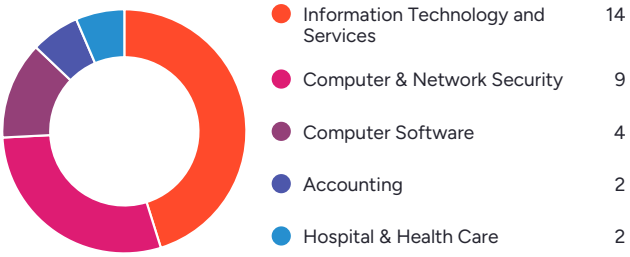
4.5 ★★★★½ (64)

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, 85% 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 90%. Wazuh - The Open Source Security Platform is also in the Endpoint Detection & Response (EDR) category.

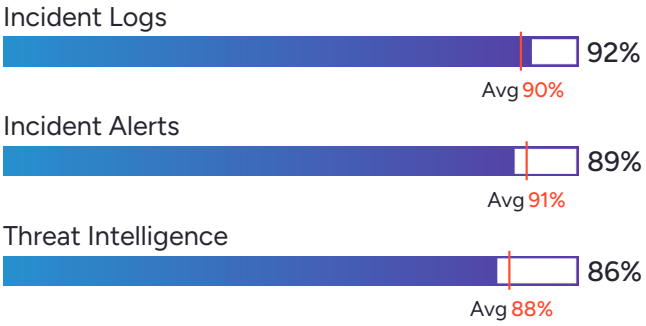
Satisfaction Ratings



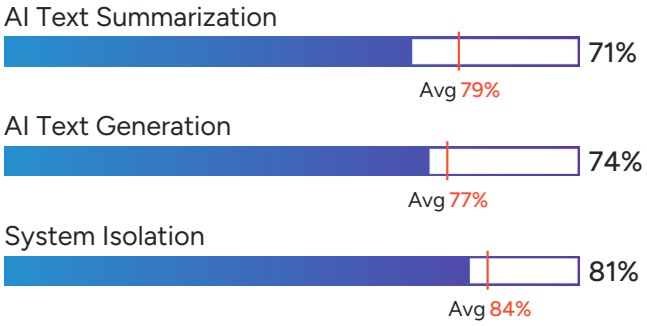
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Wazuh Inc.

HQ Location
Campbell, US

Year Founded
2015

Employees (Listed On Linkedin)
266

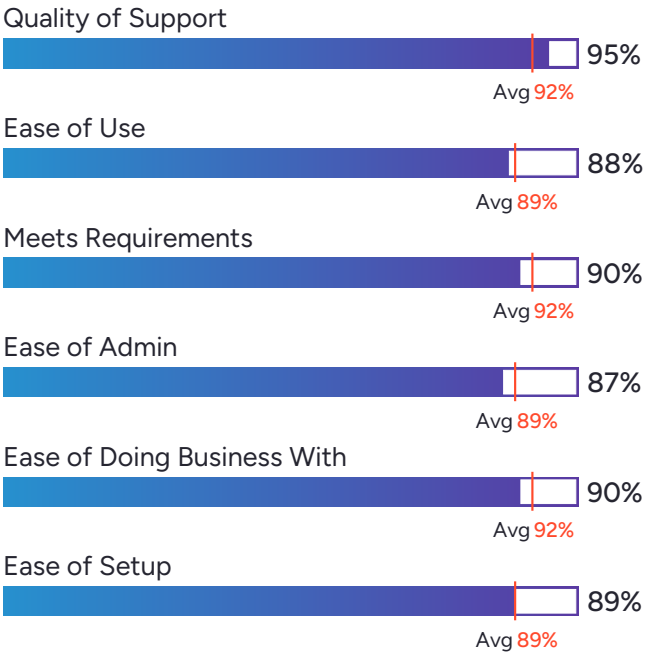
Company Website
wazuh.com

Logpoint

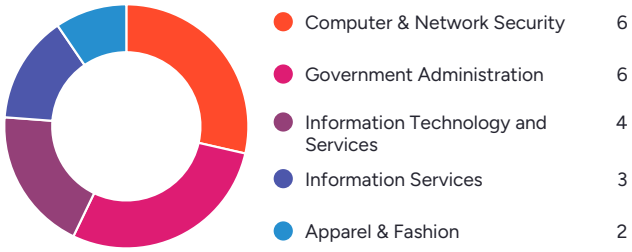
4.3 ★★★★½ (108)

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 SAP Security Software, SAP Store, User and Entity Behavior Analytics (UEBA), Security Orchestration, Automation, and Response (SOAR), Log Monitoring, Log Analysis, Security Information and Event Management (SIEM), Threat Intelligence, and Network Detection and Response (NDR) categories.

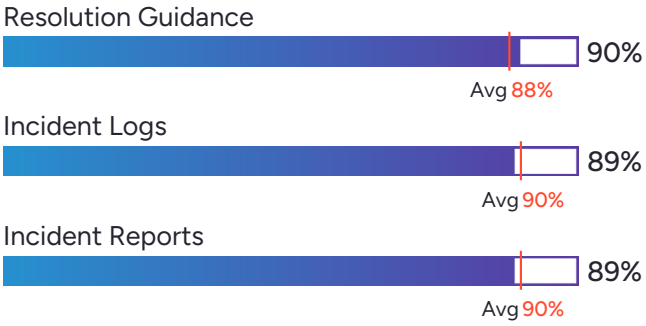
Satisfaction Ratings



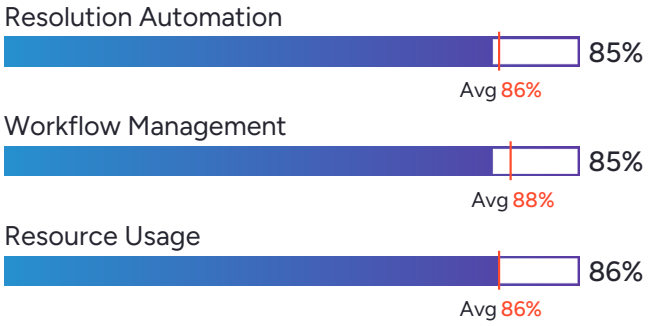
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Logpoint

HQ Location
Copenhagen, Capital Region

Year Founded
2001

Employees (Listed On Linkedin)
261

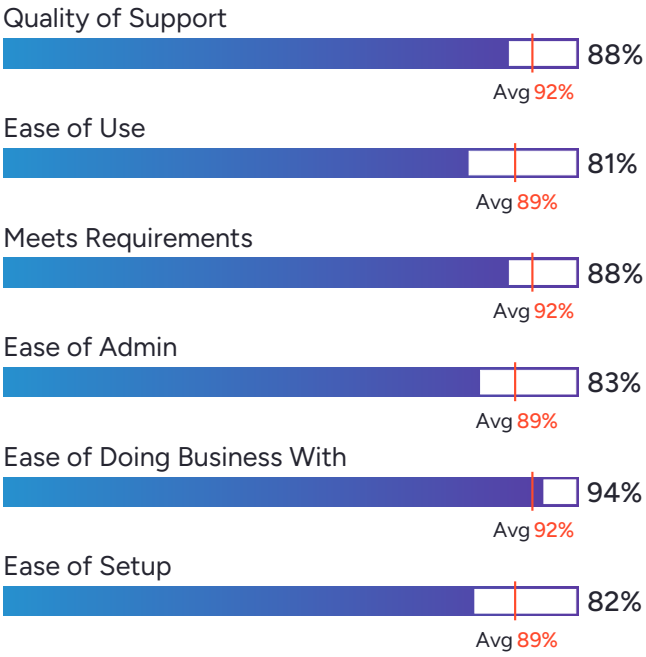
Company Website
logpoint.com

OpenCTI by Filigran

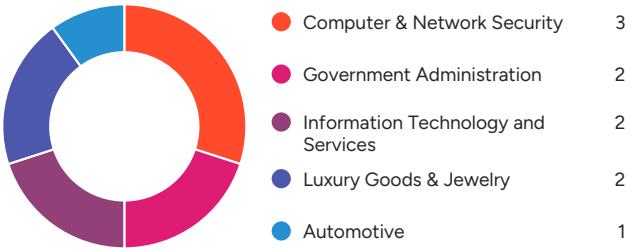
4.6 ★★★★½ (39)

OpenCTI by Filigran 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 OpenCTI by Filigran at a rate of 93%. OpenCTI by Filigran is also in the Unified Threat Management (UTM) and Threat Intelligence categories.

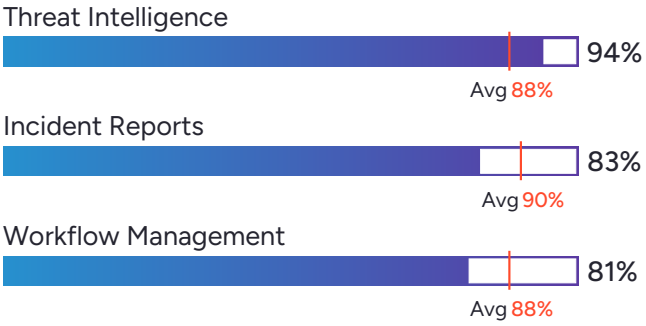
Satisfaction Ratings



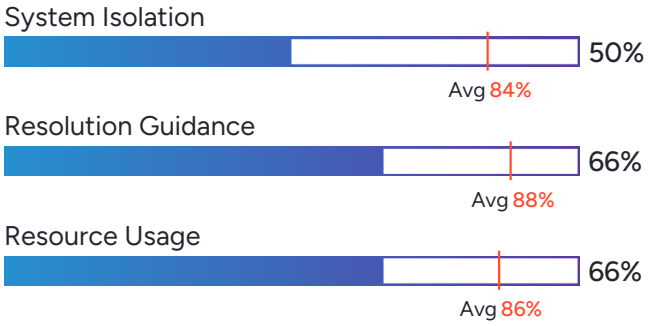
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Filigran

HQ Location
New York, US

Year Founded
2022

Employees (Listed On Linkedin)
218

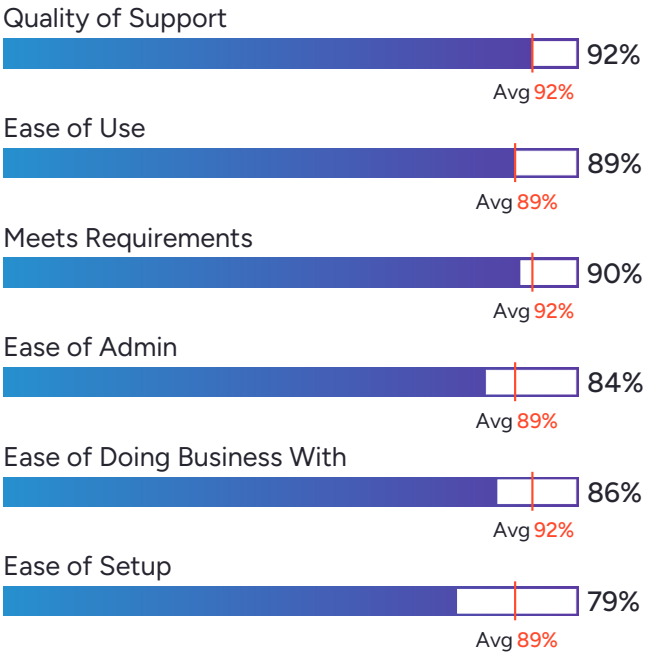
Company Website
filigran.io

D3 Security

4.2 ★★★★☆ (69)

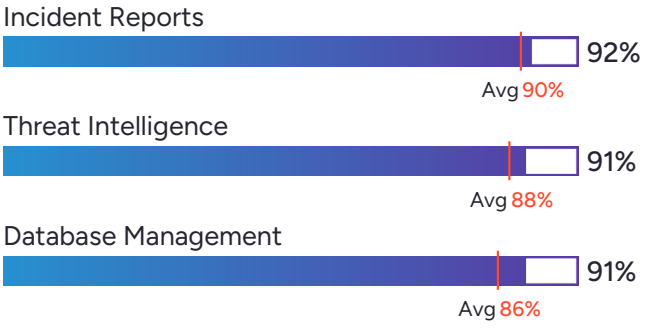
D3 Security has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 89% of users rated it 4 or 5 stars, 92% of users 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

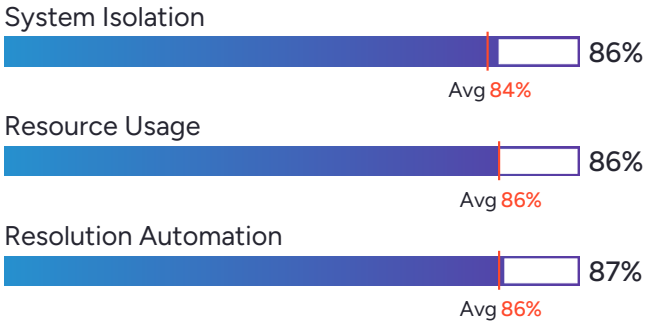


Top Industries Represented

Highest-Rated Features



Lowest-Rated Features



Ownership
D3 Security Management Systems

HQ Location
Vancouver, British Columbia

Year Founded
2012

Employees (Listed On Linkedin)
174

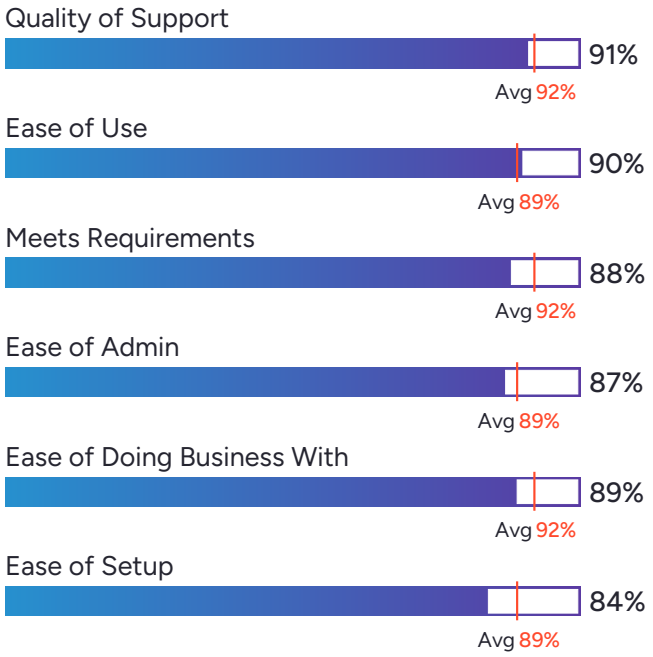
Company Website
d3security.com

Resolve

4.6 ★★★★½ (47)

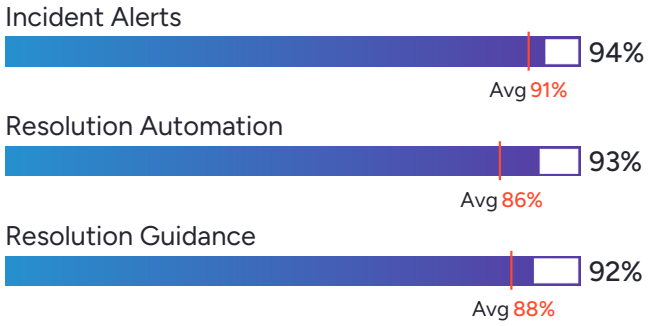
Resolve has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 93% of users rated it 4 or 5 stars, 96% of users believe 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, Runbook Automation, Network Automation Tools, Workload Automation, Robotic Process Automation (RPA), Configuration Management, AI Agents for HR, AI IT Agents, and AI Agents For Business Operations categories.

Satisfaction Ratings

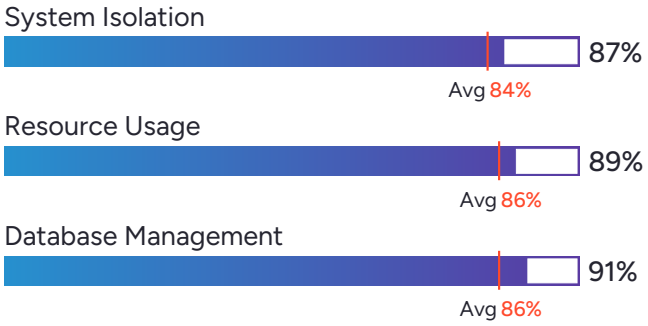


Top Industries Represented

Highest-Rated Features



Lowest-Rated Features



Ownership
Resolve

HQ Location
Campbell, California

Year Founded
2014

Employees (Listed On Linkedin)
138

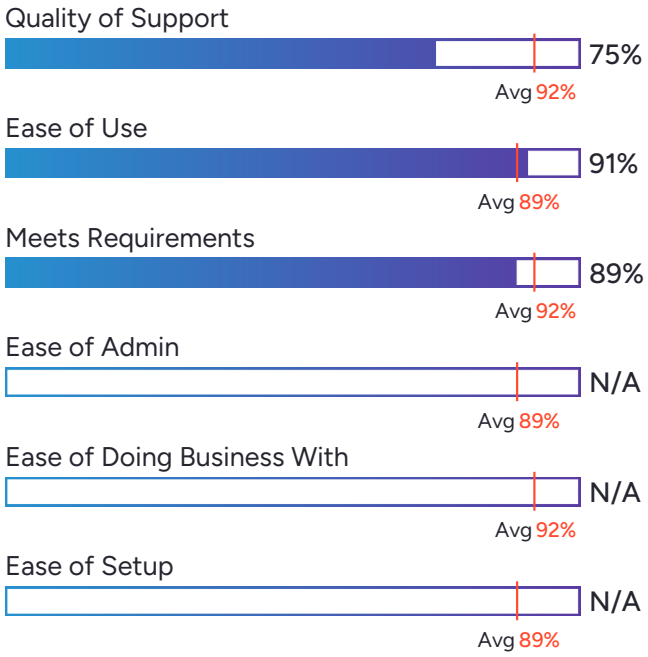
Company Website
resolve.io

Mozilla Enterprise Defense Platform

4.3 ★★★★½ (10)

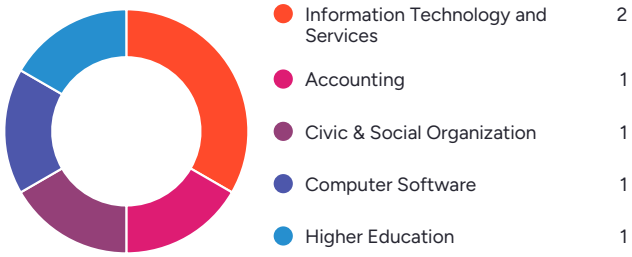
Mozilla Enterprise Defense Platform has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 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

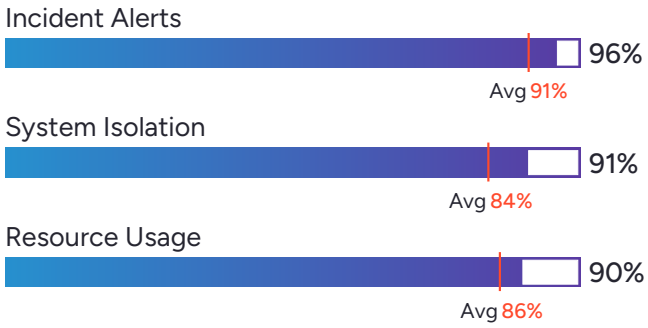


*N/A is displayed when fewer than five responses were received for the question.

Top Industries Represented



Highest-Rated Features



Lowest-Rated Features

Ownership
Mozilla

HQ Location
San Francisco, CA

Year Founded
2005

Employees (Listed On Linkedin)
1,759

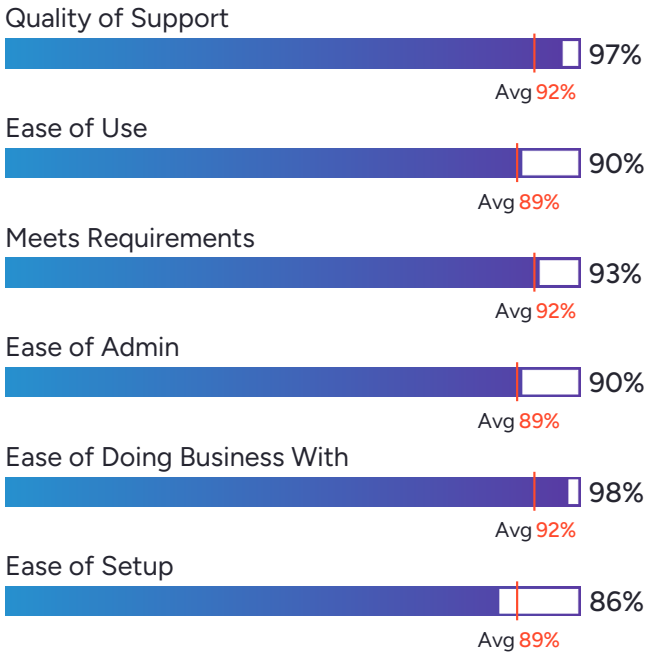
Company Website
mozilla.org

DERDACK Enterprise Alert

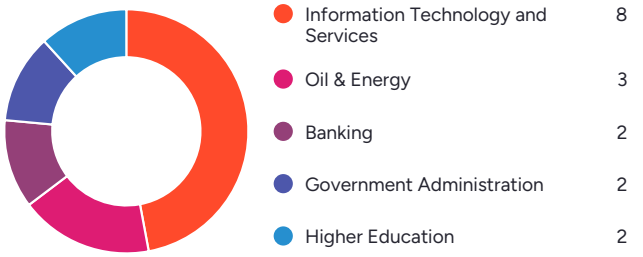
4.8 ★★★★★ (49)

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.

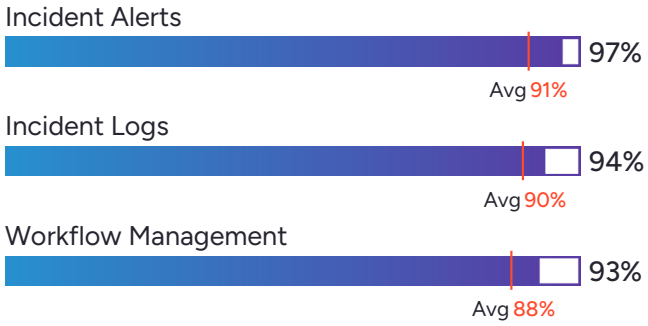
Satisfaction Ratings



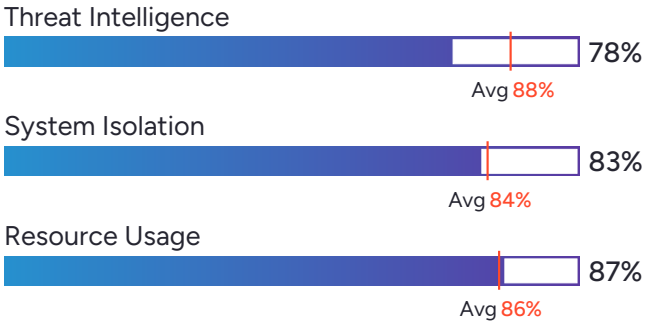
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Derdack

HQ Location
Potsdam, Germany

Year Founded
1999

Employees (Listed On Linkedin)
32

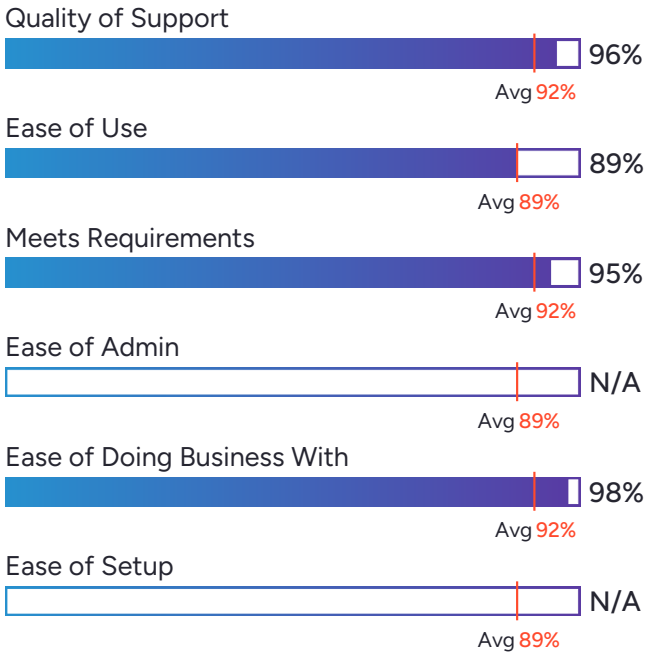
Company Website
derdack.com

Activu vis|ability

4.7 ★★★★½ (12)

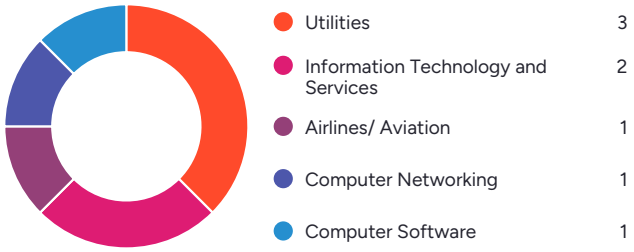
Activu vis|ability has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 4 or 5 stars, 100% 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)
90

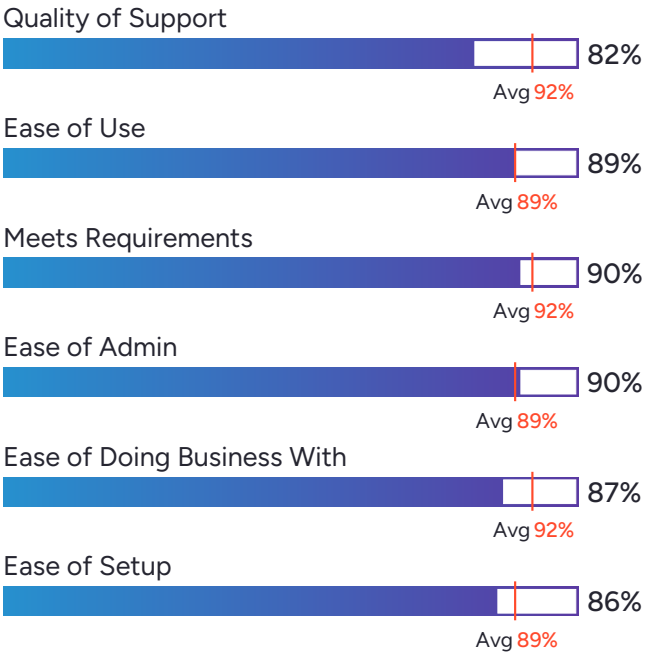
Company Website
activu.com

TheHive

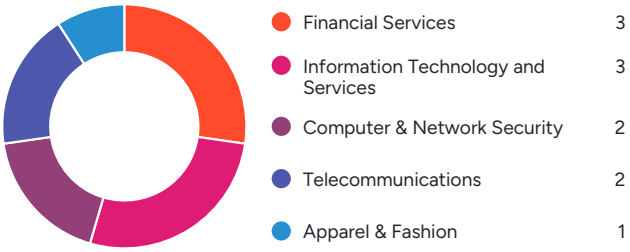
4.2 ★★★★☆ (19)

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%.

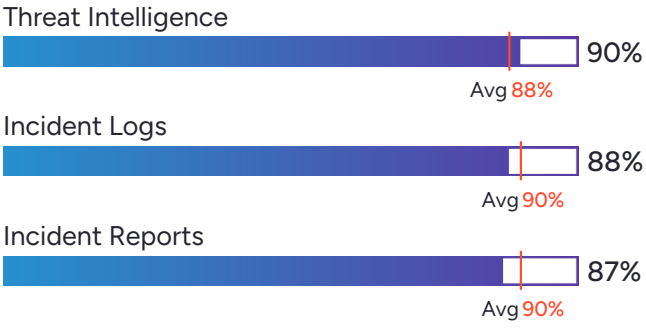
Satisfaction Ratings



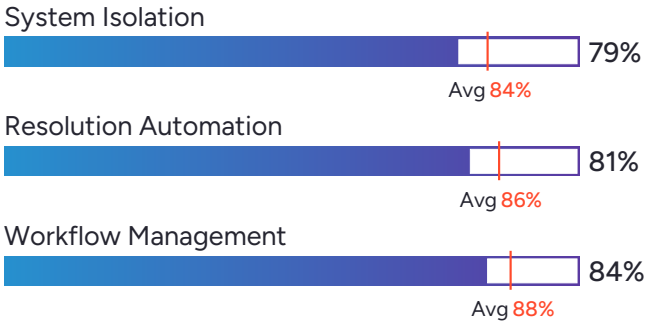
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
TheHive

HQ Location
Paris, FR

Year Founded
2018

Employees (Listed On Linkedin)
65

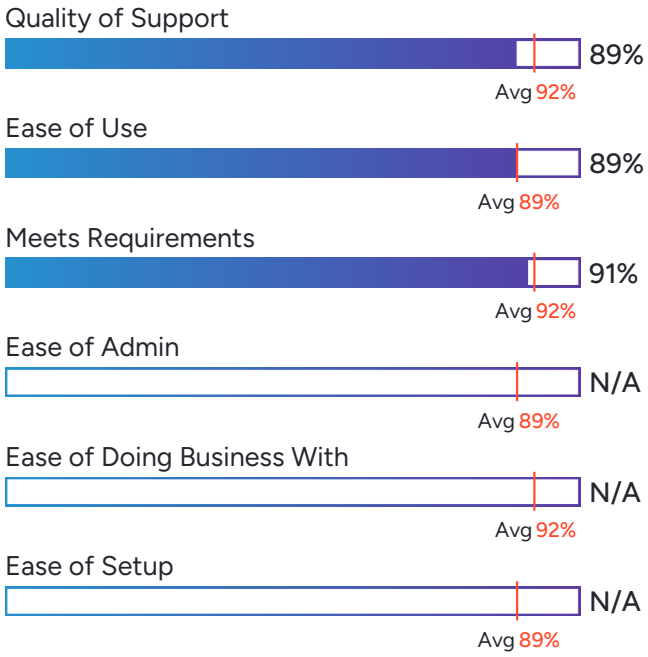
Company Website
strangebee.com

Cyber Triage

4.4 ★★★★½ (17)

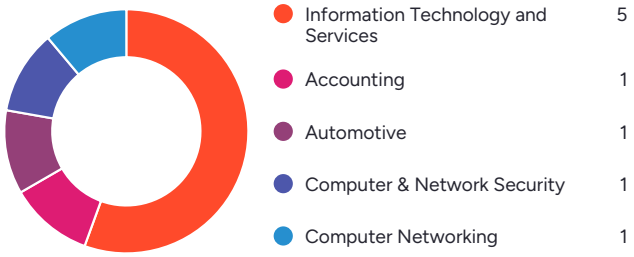
Cyber Triage has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 93% of users rated it 4 or 5 stars, 100% of users 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

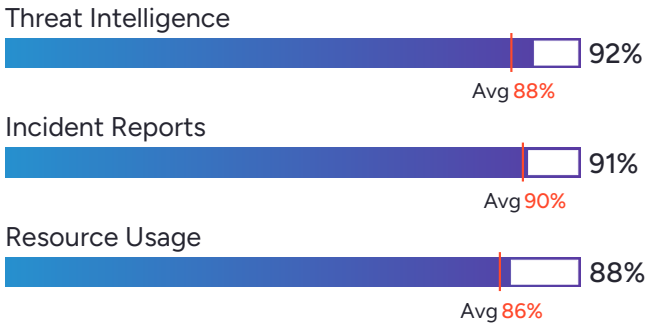


*N/A is displayed when fewer than five responses were received for the question.

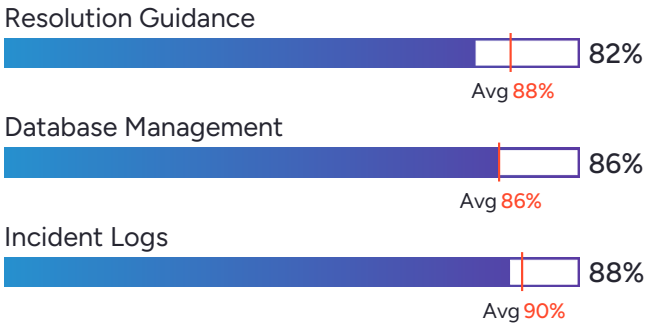
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Basis Technology

HQ Location
Somerville, US

Year Founded
1995

Employees (Listed On Linkedin)
53

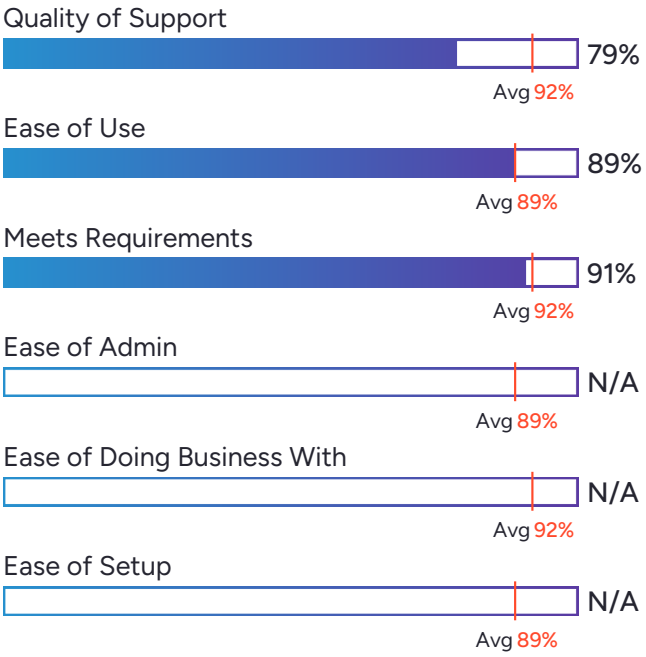
Company Website
basistech.com

ASGARD Mangement System

4.3 ★★★★½ (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%.

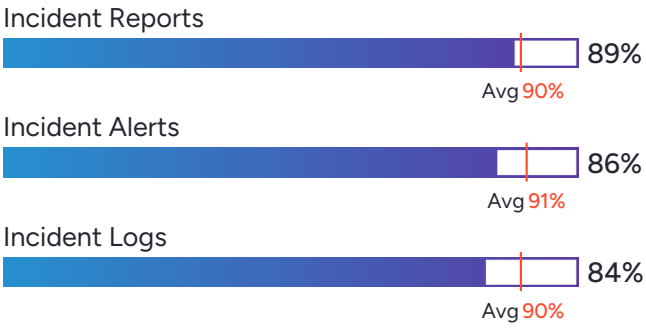
Satisfaction Ratings



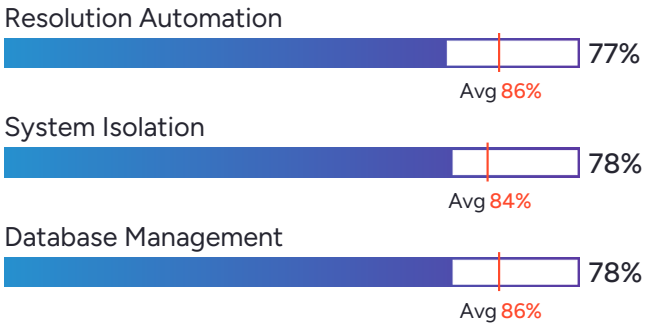
*N/A is displayed when fewer than five responses were received for the question.

Top Industries Represented

Highest-Rated Features



Lowest-Rated Features



Ownership
Nextron Systems

HQ Location
Dietzenbach, Hessen

Year Founded
2017

Employees (Listed On Linkedin)
48

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%	94%	93%	87%	90%	73
Datadog	89%	96%	93%	86%	90%	88%	85%	86%	66
IBM Instana	85%	81%	83%	82%	81%	85%	93%	87%	51
Torq	98%	100%	98%	96%	100%	97%	97%	96%	96
Cynet	96%	97%	94%	95%	98%	94%	95%	93%	89
Dynatrace	92%	92%	90%	88%	90%	91%	86%	86%	75
Tines	96%	97%	93%	94%	99%	97%	94%	95%	89
ServiceNow Security Operations	87%	90%	94%	81%	89%	91%	81%	83%	47
Sumo Logic	88%	88%	91%	88%	88%	88%	86%	85%	64
Barracuda Incident Response	91%	92%	93%	97%	92%	94%	97%	97%	73
SpinOne	97%	100%	98%	93%	96%	98%	94%	90%	94
CYREBRO	87%	91%	86%	91%	89%	86%	84%	89%	54
OneTrust Tech Risk & Compliance	93%	93%	93%	96%	97%	97%	92%	91%	81
Pondurance	94%	100%	97%	93%	96%	97%	94%	91%	72
Blumira Automated Detection & Response	94%	100%	92%	94%	97%	97%	94%	93%	85
UnderDefense MAXI	95%	100%	97%	94%	98%	100%	94%	96%	84

(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	
Splunk On-Call	95%	93%	95%	91%	100%	94%	94%	91%	80
Belkasoft	90%	100%	92%	N/A	N/A	97%	93%	92%	63
Intezer	89%	93%	88%	90%	86%	93%	98%	93%	66
Defendify All-In-One Cybersecurity Solution	96%	94%	93%	98%	99%	98%	94%	94%	92
SIRP	94%	90%	96%	100%	100%	99%	98%	96%	81
Palo Alto Cortex XSIAM	87%	89%	87%	84%	88%	85%	83%	85%	54
Resolver	88%	87%	85%	75%	91%	93%	76%	81%	53
InsightIDR	89%	90%	90%	88%	89%	90%	86%	90%	61
Proofpoint Threat Defense	91%	86%	89%	93%	93%	89%	95%	89%	75
Splunk SOAR (Security Orchestration, Automation and Response)	88%	83%	88%	84%	90%	91%	82%	84%	54
Darktrace / NETWORK	89%	91%	94%	73%	93%	93%	88%	73%	68
Splunk Synthetic Monitoring	90%	100%	93%	N/A	N/A	95%	N/A	93%	75
Proofpoint Threat Response Auto-Pull	89%	95%	93%	89%	89%	90%	86%	89%	62
LevelBlue USM Anywhere	91%	88%	93%	85%	91%	91%	81%	88%	71
LogRhythm SIEM	87%	89%	88%	83%	90%	88%	83%	88%	54
Wazuh - The Open Source Security Platform	90%	85%	90%	89%	89%	82%	83%	87%	66

(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	
Logpoint	91%	100%	90%	87%	90%	95%	89%	88%	71
OpenCTI by Filigran	93%	100%	88%	83%	94%	88%	82%	81%	83
D3 Security	84%	92%	90%	84%	86%	92%	79%	89%	39
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
DERDACK Enterprise Alert	97%	100%	93%	90%	98%	97%	86%	90%	93
Activu vis|ability	94%	100%	95%	N/A	98%	96%	N/A	89%	83
TheHive	85%	88%	90%	90%	87%	82%	86%	89%	42
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	91%	93%	92%	89%	92%	92%	89%	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	90%	88%	82%	86%
Torq	92%	92%	86%	91%
Cynet	95%	93%	92%	93%
Dynatrace	78%	83%	73%	80%
Tines		93%	79%	87%
ServiceNow Security Operations	90%	90%	90%	90%
Sumo Logic	81%	85%	78%	80%
Barracuda Incident Response	91%	90%	93%	89%
SpinOne	90%	91%	93%	93%
CYREBRO	84%	86%	78%	88%
OneTrust Tech Risk & Compliance	N/A	N/A	N/A	N/A
Pondurance	93%	92%	92%	95%
Blumira Automated Detection & Response	87%	94%	86%	92%
UnderDefense MAXI	95%	97%	91%	98%

(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
Splunk On-Call	N/A	N/A	N/A	N/A
Belkasoft	80%	95%	82%	89%
Intezer	N/A	N/A	N/A	N/A
Defendify All-In-One Cybersecurity Solution	N/A	93%	N/A	93%
SIRP	91%	97%	96%	98%
Palo Alto Cortex XSIAM	80%	82%	79%	85%
Resolver	69%	75%	71%	66%
InsightIDR	88%	89%	88%	93%
Proofpoint Threat Defense	84%	86%	81%	86%
Splunk SOAR (Security Orchestration, Automation and Response)	88%	87%	85%	90%
Darktrace / NETWORK	90%	90%	100%	86%
Splunk Synthetic Monitoring	84%	92%	89%	84%
Proofpoint Threat Response Auto-Pull	92%	78%	74%	86%
LevelBlue USM Anywhere	88%	90%	92%	93%
LogRhythm SIEM	84%	86%	83%	89%
Wazuh - The Open Source Security Platform	82%	82%	81%	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
Logpoint	85%	90%	88%	87%
OpenCTI by Filigran	73%	66%	50%	94%
D3 Security	87%		86%	91%
Resolve	93%	92%	87%	91%
Mozilla Enterprise Defense Platform	88%	84%	91%	86%
DERDACK Enterprise Alert	89%	90%	83%	78%
Activu vis|ability	89%	89%	N/A	N/A
TheHive	81%	84%	79%	90%
Cyber Triage		82%		92%
ASGARD Mangement System	77%	80%	78%	84%
Average	86%	87%	84%	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	86%	86%	84%
Datadog	93%	91%	87%
IBM Instana	90%	90%	86%
Torq	83%	86%	83%
Cynet	92%	92%	91%
Dynatrace	87%	86%	90%
Tines	93%	89%	88%
ServiceNow Security Operations	91%	89%	90%
Sumo Logic	90%	86%	86%
Barracuda Incident Response	88%	88%	86%
SpinOne	95%	95%	94%
CYREBRO	88%	85%	84%
OneTrust Tech Risk & Compliance	91%	91%	91%
Pondurance	95%	94%	89%
Blumira Automated Detection & Response	91%	89%	91%
UnderDefense MAXI	100%	99%	96%

(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
Splunk On-Call	N/A	N/A	N/A
Belkasoft	92%	95%	82%
Intezer	N/A	N/A	N/A
Defendify All-In-One Cybersecurity Solution	N/A	92%	94%
SIRP	96%	96%	91%
Palo Alto Cortex XSIAM	89%	86%	84%
Resolver	87%	83%	77%
InsightIDR	93%	91%	86%
Proofpoint Threat Defense	87%	89%	83%
Splunk SOAR (Security Orchestration, Automation and Response)	90%	92%	84%
Darktrace / NETWORK	86%	91%	74%
Splunk Synthetic Monitoring	92%	90%	78%
Proofpoint Threat Response Auto-Pull	88%	91%	
LevelBlue USM Anywhere	93%	93%	92%
LogRhythm SIEM	90%	90%	90%
Wazuh - The Open Source Security Platform	92%	84%	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
Logpoint	89%	89%	86%
OpenCTI by Filigran	79%	83%	66%
D3 Security		92%	86%
Resolve	N/A	N/A	89%
Mozilla Enterprise Defense Platform	86%	88%	90%
DERDACK Enterprise Alert	94%	88%	87%
Activu vis|ability	N/A	N/A	N/A
TheHive	88%	87%	84%
Cyber Triage	88%	91%	88%
ASGARD Mangement System	84%	89%	79%
Average	90%	90%	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	87%	82%	86%
Datadog	94%	86%	
IBM Instana	95%	88%	88%
Torq	96%	82%	96%
Cynet	96%	91%	92%
Dynatrace	90%	85%	86%
Tines	94%	86%	93%
ServiceNow Security Operations	92%	90%	94%
Sumo Logic	88%	83%	85%
Barracuda Incident Response	89%	88%	88%
SpinOne	94%	94%	95%
CYREBRO	90%	83%	84%
OneTrust Tech Risk & Compliance	N/A	N/A	N/A
Pondurance	95%	90%	86%
Blumira Automated Detection & Response	94%	83%	88%
UnderDefense MAXI	99%	94%	96%

(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
Splunk On-Call	N/A	N/A	N/A
Belkasoft	84%	80%	91%
Intezer	N/A	N/A	N/A
Defendify All-In-One Cybersecurity Solution	93%	N/A	N/A
SIRP	95%	90%	94%
Palo Alto Cortex XSIAM	88%	84%	85%
Resolver	80%	83%	85%
InsightIDR	91%	89%	88%
Proofpoint Threat Defense	89%	86%	93%
Splunk SOAR (Security Orchestration, Automation and Response)	90%	83%	87%
Darktrace / NETWORK	89%	80%	80%
Splunk Synthetic Monitoring	89%	84%	81%
Proofpoint Threat Response Auto-Pull	95%	78%	78%
LevelBlue USM Anywhere	95%	86%	90%
LogRhythm SIEM	90%	89%	88%
Wazuh - The Open Source Security Platform	89%	82%	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.

Management

	Incident Alerts	Database Management	Workflow Management
Logpoint	88%	86%	85%
OpenCTI by Filigran	79%		81%
D3 Security		91%	91%
Resolve	94%	91%	N/A
Mozilla Enterprise Defense Platform	96%	88%	88%
DERDACK Enterprise Alert	97%	90%	93%
Activu vis|ability	N/A	N/A	N/A
TheHive	86%	86%	84%
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%	75%	14%
Datadog	18%	49%	34%
IBM Instana	16%	47%	38%
Torq	28%	57%	15%
Cynet	34%	53%	13%
Dynatrace	10%	30%	60%
Tines	21%	36%	44%
ServiceNow Security Operations	19%	10%	71%
Sumo Logic	16%	50%	33%
Barracuda Incident Response	20%	53%	27%
SpinOne	57%	37%	6%
CYREBRO	27%	60%	13%
OneTrust Tech Risk & Compliance	48%	37%	15%
Pondurance	9%	64%	27%
Blumira Automated Detection & Response	33%	59%	8%
UnderDefense MAXI	15%	69%	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 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.)
Splunk On-Call	7%	53%	40%
Belkasoft	77%	15%	8%
Intezer	50%	28%	22%
Defendify All-In-One Cybersecurity Solution	82%	18%	0%
SIRP	45%	27%	27%
Palo Alto Cortex XSIAM	18%	28%	54%
Resolver	13%	30%	57%
InsightIDR	19%	53%	27%
Proofpoint Threat Defense	25%	50%	25%
Splunk SOAR (Security Orchestration, Automation and Response)	21%	46%	33%
Darktrace / NETWORK	6%	88%	6%
Splunk Synthetic Monitoring	50%	25%	25%
Proofpoint Threat Response Auto-Pull	4%	33%	63%
LevelBlue USM Anywhere	15%	67%	19%
LogRhythm SIEM	18%	43%	39%
Wazuh - The Open Source Security Platform	43%	38%	19%

(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.)
Logpoint	23%	48%	30%
OpenCTI by Filigran	0%	50%	50%
D3 Security	24%	30%	46%
Resolve	17%	50%	33%
Mozilla Enterprise Defense Platform	40%	40%	20%
DERDACK Enterprise Alert	10%	28%	62%
Activu vis|ability	50%	33%	17%
TheHive	11%	39%	50%
Cyber Triage	40%	13%	47%
ASGARD Mangement System	23%	38%	38%
Average	26%	43%	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%	15%	3%	3%	75	25
Datadog	91%	9%	2.8	86%	7%	5%	2%	37	15
IBM Instana	83%	17%	4.2	82%	9%	9%	0%	17	18
Torq	100%	0%	1.2	69%	23%	0%	8%	7	17
Cynet	78%	22%	1.2	64%	23%	3%	10%	17	19
Dynatrace	61%	39%	2.8	67%	30%	2%	1%	75	24
Tines	92%	8%	1.1	81%	14%	5%	0%	7	15
ServiceNow Security Operations	33%	67%	4.3	40%	20%	20%	20%	N/A	N/A
Sumo Logic	78%	22%	1.7	72%	14%	3%	11%	17	14
Barracuda Incident Response	78%	22%	3.6	78%	0%	0%	22%	3	14
SpinOne	85%	15%	0.4	59%	15%	7%	19%	7	13
CYREBRO	72%	28%	1.8	57%	27%	5%	11%	3	18
OneTrust Tech Risk & Compliance	67%	33%	2.2	89%	0%	0%	11%	N/A	N/A
Pondurance	78%	22%	1.2	50%	38%	0%	13%	7	23
Blumira Automated Detection & Response	85%	15%	0.5	83%	8%	3%	8%	3	10
UnderDefense MAXI	80%	20%	N/A	80%	20%	0%	0%	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 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)
Splunk On-Call	90%	10%	1.0	82%	0%	0%	18%	27	9
Belkasoft	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Intezer	33%	67%	N/A	80%	0%	0%	20%	N/A	N/A
Defendify All-In-One Cybersecurity Solution	80%	20%	0.3	90%	0%	0%	10%	N/A	10
SIRP	63%	38%	0.9	0%	100%	0%	0%	17	14
Palo Alto Cortex XSIAM	30%	70%	3.6	50%	30%	9%	11%	17	24
Resolver	83%	17%	6.4	57%	32%	0%	11%	125	24
InsightIDR	83%	17%	3.6	65%	12%	12%	12%	7	14
Proofpoint Threat Defense	80%	20%	1.0	33%	50%	0%	17%	17	19
Splunk SOAR (Security Orchestration, Automation and Response)	43%	57%	N/A	60%	20%	20%	0%	N/A	N/A
Darktrace / NETWORK	30%	70%	1.8	0%	100%	0%	0%	7	33
Splunk Synthetic Monitoring	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Proofpoint Threat Response Auto-Pull	21%	79%	1.0	39%	56%	0%	6%	191	15
LevelBlue USM Anywhere	50%	50%	1.6	75%	19%	6%	0%	3	16
LogRhythm SIEM	27%	73%	2.4	32%	37%	14%	17%	7	22
Wazuh - The Open Source Security Platform	46%	54%	2.3	85%	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)
Logpoint	5%	95%	1.8	45%	20%	10%	25%	7	15
OpenCTI by Filigran	50%	50%	5.1	71%	14%	14%	0%	37	12
D3 Security	20%	80%	N/A	N/A	N/A	N/A	N/A	N/A	N/A
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
DERDACK Enterprise Alert	32%	68%	2.8	82%	12%	6%	0%	75	14
Activu vis|ability	N/A	N/A	N/A	0%	60%	40%	0%	N/A	N/A
TheHive	38%	62%	2.7	89%	11%	0%	0%	27	10
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	78%	12
Datadog	61%	10
IBM Instana	57%	9
Torq	43%	4
Cynet	83%	12
Dynatrace	53%	19
Tines	64%	6
ServiceNow Security Operations	N/A	19
Sumo Logic	58%	11
Barracuda Incident Response	77%	20
SpinOne	78%	11
CYREBRO	75%	15
OneTrust Tech Risk & Compliance	59%	N/A
Pondurance	81%	8
Blumira Automated Detection & Response	65%	12
UnderDefense MAXI	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)
Splunk On-Call	70%	16
Belkasoft	N/A	N/A
Intezer	N/A	N/A
Defendify All-In-One Cybersecurity Solution	74%	14
SIRP	75%	N/A
Palo Alto Cortex XSIAM	65%	22
Resolver	73%	16
InsightIDR	75%	11
Proofpoint Threat Defense	64%	13
Splunk SOAR (Security Orchestration, Automation and Response)	N/A	N/A
Darktrace / NETWORK	69%	9
Splunk Synthetic Monitoring	N/A	N/A
Proofpoint Threat Response Auto-Pull	91%	18
LevelBlue USM Anywhere	83%	20
LogRhythm SIEM	62%	16
Wazuh - The Open Source Security Platform	47%	12

(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)
Logpoint	53%	23
OpenCTI by Filigran	46%	0
D3 Security	N/A	N/A
Resolve	53%	N/A
Mozilla Enterprise Defense Platform	N/A	N/A
DERDACK Enterprise Alert	67%	12
Activu vis|ability	N/A	N/A
TheHive	84%	23
Cyber Triage	N/A	N/A
ASGARD Mangement System	N/A	N/A
Average	67%	13

(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	2,387	320,565
Datadog	Datadog	2010	10,625	494,121
IBM Instana	IBM	1911	339,241	18,990,065
Torq	torq	2020	393	35,600
Cynet	Cynet	2014	329	41,084
Dynatrace	Dynatrace	2005	5,800	389,995
Tines	Tines	2018	538	56,847
ServiceNow Security Operations	ServiceNow	2004	31,344	1,401,182
Sumo Logic	Sumo Logic	2010	808	163,809
Barracuda Incident Response	Barracuda	2002	2,229	80,285
SpinOne	SpinAI	2017	91	4,037
CYREBRO	CYREBRO	2013	99	12,071
OneTrust Tech Risk & Compliance	OneTrust	2016	2,543	380,039
Pondurance	Pondurance	2008	119	23,726
Blumira Automated Detection & Response	Blumira	2018	67	7,676
UnderDefense MAXI	UnderDefense	2017	134	6,560

(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
Splunk On-Call	Cisco	1984	95,386	7,277,442
Belkasoft	Belkasoft	2002	35	26,078
Intezer	Intezer	2015	82	11,589
Defendify All-In-One Cybersecurity Solution	Defendify	2017	40	2,625
SIRP	SIRP	2017	59	5,994
Palo Alto Cortex XSIAM	Palo Alto Networks	2005	18,396	1,780,857
Resolver	Resolver		727	32,320
InsightIDR	Rapid7	2000	3,249	214,542
Proofpoint Threat Defense	Proofpoint	2002	5,020	185,826
Splunk SOAR (Security Orchestration, Automation and Response)	Cisco	1984	95,386	7,277,442
Darktrace / NETWORK	Darktrace	2013	2,537	242,360
Splunk Synthetic Monitoring	Cisco	1984	95,386	7,277,442
Proofpoint Threat Response Auto-Pull	Proofpoint	2002	5,020	185,826
LevelBlue USM Anywhere	LevelBlue		638	112,936
LogRhythm SIEM	Exabeam	2013	819	49,506
Wazuh - The Open Source Security Platform	Wazuh Inc.	2015	266	73,072

(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
Logpoint	Logpoint	2001	261	30,966
OpenCTI by Filigran	Filigran	2022	218	17,269
D3 Security	D3 Security Management Systems	2012	174	21,453
Resolve	Resolve	2014	138	20,244
Mozilla Enterprise Defense Platform	Mozilla	2005	1,759	442,159
DERDACK Enterprise Alert	Derdack	1999	32	705
Activu vis|ability	Activu	1983	90	2,858
TheHive	TheHive	2018	65	7,862
Cyber Triage	Basis Technology	1995	53	9,753
ASGARD Mangement System	Nextron Systems	2017	48	4,490

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