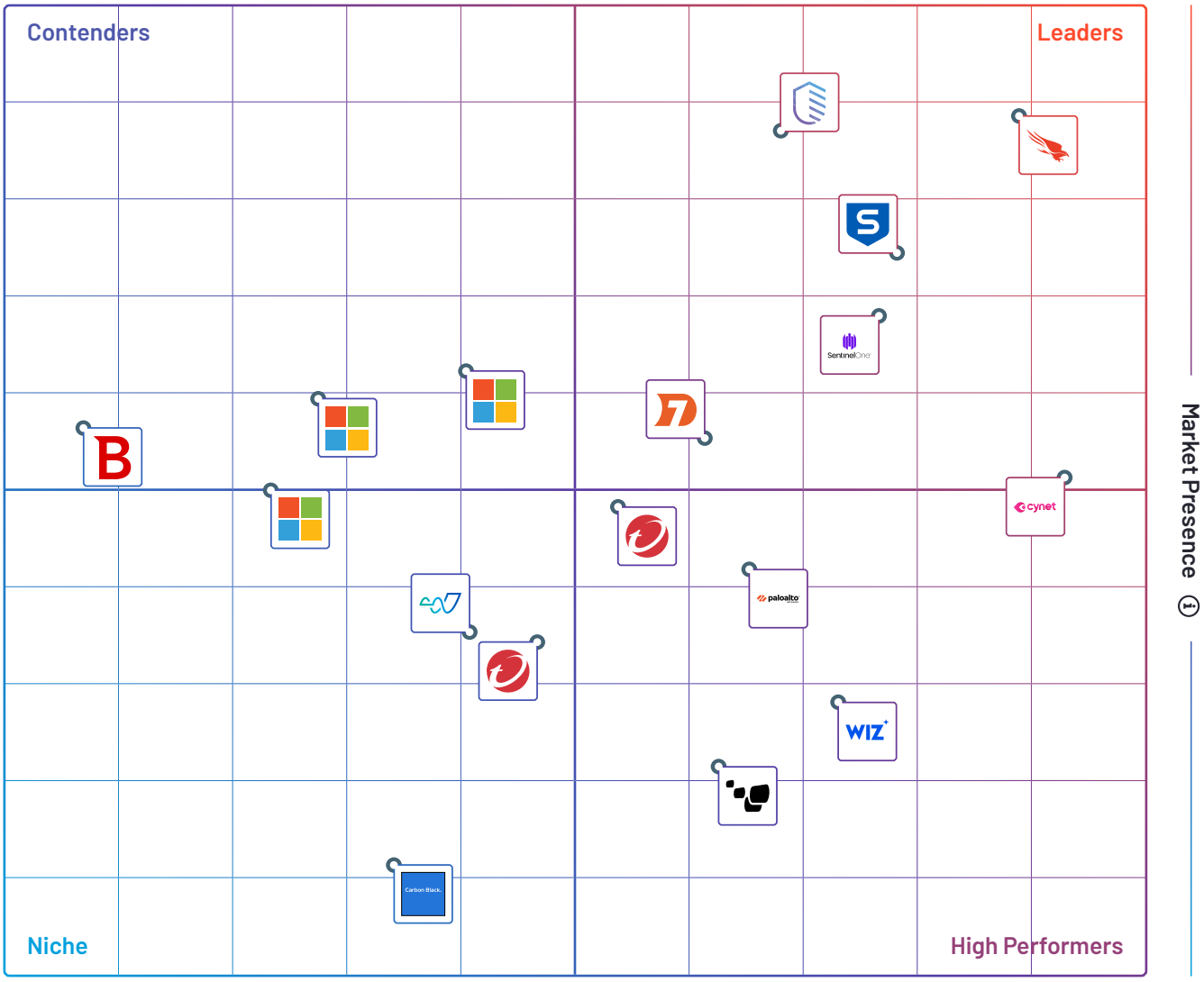
Grid® Report for Extended Detection and Response (XDR) Platforms | Fall 2022

Extended Detection and Response (XDR) Platforms



G2 Grid® Scoring

(Extended Detection and Response (XDR) Platforms continues on next page)

Extended Detection and Response (XDR) Platforms (continued)

Extended Detection and Response (XDR) Platforms Definition

Extended detection and response (XDR) platforms are tools used to automate the discovery and remediation of security issues across hybrid systems. These tools are capable of performing detection and response related to networks, endpoints, cloud services, and applications. Companies are adopting these technologies because most traditional detection and response solutions are limited to a single medium such as endpoint security or network security while XDR is capable of securing complex hybrid environments.

XDR solutions provide a single system for managing security issues as they arise regardless of the source within the organization. They can also be used to consolidate redundant, similar detection and response technologies and simplify detection and remediation for security teams.

Endpoint detection & response (EDR) software and network detection and response (NDR) software operate similarly, but most are limited to their specific medium. For example, many NDR solutions can analyze and resolve issues on a local business network, but cannot support detection and response for cloud workloads or remote endpoints. While numerous families of detection and response solutions have emerged in recent years, XDR is capable of extending security across networks, endpoints, cloud services, and virtual environments.

To qualify for inclusion in the Extended Detection and Response (XDR) category, a product must:

- Analyze network, cloud, and endpoint activity continuously
- Utilize artificial intelligence (AI) or machine learning (ML) to develop baselines for system behaviors
- Automate threat and anomaly detection across the hybrid environments
- Deploy forensics upon detection for investigation and remediation

Extended Detection and Response (XDR) Platforms Grid® Scoring Description

Products shown on the Grid® for Extended Detection and Response (XDR) Platforms have received a minimum of 10 reviews/ratings in data gathered by August 30, 2022. 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: Crowdstrike Falcon Endpoint Protection Platform, IBM Security QRadar, Sophos Intercept X: Next-Gen Endpoint, SentinelOne Singularity, Cynet 360 AutoXDR™, and InsightIDR
- High Performing products have high customer Satisfaction scores and low Market Presence compared to the rest of the category. High Performers include: Cortex XDR, Trend Micro Apex One, Wiz, and ExtraHop
- 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: Microsoft 365 Defender, Microsoft Threat Protection, and Bitdefender GravityZone
- 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: Trend Micro Vision One (XDR), LogRhythm NextGen SIEM Platform, Microsoft Defender for Cloud, and VMware Carbon Black Cloud

Grid® Scores for Extended Detection and Response (XDR) Platforms

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
Crowdstrike Falcon Endpoint Protection Platform	64	91	93	92
IBM Security QRadar	50	69	91	80
Sophos Intercept X: Next-Gen Endpoint	79	80	77	79
SentinelOne	40	78	70	74
Cynet 360 AutoXDR™	76	96	52	74
InsightIDR	37	62	56	59

High Performers

Cortex XDR	31	66	41	54
Trend Micro	49	54	48	51
Wiz	11	75	26	50
ExtraHop	22	63	18	41

Contenders

Microsoft 365 Defender	18	40	64	52
Microsoft Threat Protection	14	26	61	43
Bitdefender GravityZone	21	4	57	31

(Extended Detection and Response (XDR) Platforms 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 Extended Detection and Response (XDR) Platforms (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
Trend Micro Vision One (XDR)	21	46	33	39
LogRhythm	53	40	34	37
Microsoft Defender for Cloud	12	22	50	36
VMware Carbon Black Cloud Endpoint	22	33	7	20

* 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 Extended Detection and Response (XDR) Platforms category algorithmically based on data sourced from product reviews shared by G2 users and data aggregated from online sources and social networks.

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

G2 rates products and sellers based on reviews gathered from our user community, as well as data aggregated from online sources and social networks. We apply a unique algorithm (v3.0) to this data to calculate the Satisfaction and Market Presence scores in real time. The Grid® Report for Extended Detection and Response (XDR) Platforms | Fall 2022 is based on scores calculated using the G2 algorithm v3.0 from reviews collected through August 30, 2022. To view the Extended Detection and Response (XDR) Platforms Grid® with the most recent data, please visit the Extended Detection and Response (XDR) Platforms page.

Satisfaction

The Satisfaction rating is affected by the following (in order of importance):

- Customer satisfaction with end user-focused product attributes based on user reviews
- Popularity and statistical significance based on the number of reviews received by G2
- Quality of reviews received (reviews that are more thoroughly completed will be weighted more heavily)
- Age of reviews (more-recent reviews provide relevant and up-to-date information that is reflective of the current state of a product)
- Customers' satisfaction with administration-specific product attributes based on user reviews
- Overall customer satisfaction and Net Promoter Score® (NPS) based on ratings by G2 users

Note: The customer satisfaction score is normalized for each Grid®, meaning the scores are relative.

(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)

Market Presence

The Market Presence score is affected by the following (in order of importance):

- Market presence is a combination of 15 metrics from G2's reviews, publicly available information, and third-party sources
- Both the software sellers and the individual products are measured on various criteria. The criteria are listed in order of importance. Products metric receive greater weight than seller metrics

Criteria	Measured For		Metrics
	Product	Seller	
Number of Employees	✓	✓	Employee Count (based on social networks and public sources)
Reviews	✓		Review Count (weighted by recency)
Web Presence	✓	✓	
Social Presence	✓	✓	
Growth	✓	✓	Employee Growth, Web Presence Growth
Seller Age		✓	
Employee Satisfaction and Engagement		✓	

- Each input is normalized by category and segment. This means that scores are relative to other products in the category/segment and may change from segment to segment
- The scores are then scaled from 0-100

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.

(Grid® Methodology continues on next page)

Grid® Methodology (continued)

Rating Changes and Dynamics

The ratings in this report are based on a snapshot of the user reviews and social data collected by G2 up through August 30, 2022. 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. We require the use of a LinkedIn account or verified business email address to validate a G2 user's identity and employer. We also validate users by partnering with sellers and organizations to securely authenticate users through select platforms. We do not allow users to review their current or former employers' products, or those of their employers' competitors. Additionally, all reviews are manually checked by our team after our algorithm filters out reviews that don't meet our submission requirements. All reviews must pass our moderation process before they are published.

Our G2 staff does not add any subjective input to the ratings, which are determined algorithmically based on data aggregated from publicly available online sources and social networks. Sellers cannot influence their ratings by spending time or money with us. Only the opinion of real users and data from public sources factor into the ratings.

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 Extended Detection and Response (XDR) Platforms category.

Product Profiles

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

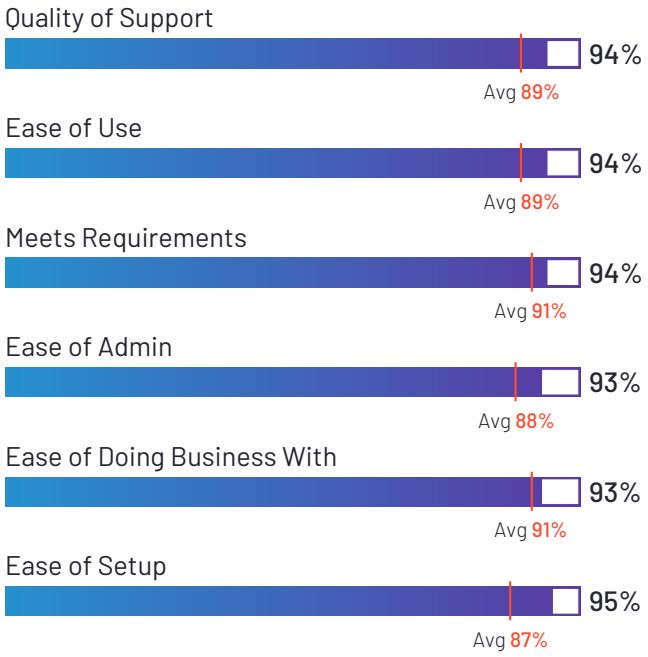
Crowdstrike Falcon Endpoint Protection Platform

4.7 ★★★★½ (159)

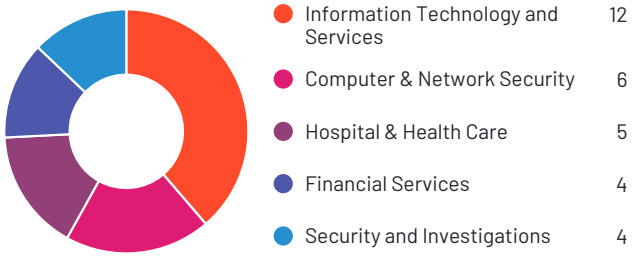
Leader FALL 2022

Crowdstrike Falcon Endpoint Protection Platform has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. Crowdstrike Falcon Endpoint Protection Platform has the largest Market Presence among products in Extended Detection and Response (XDR) Platforms. 100% 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 Crowdstrike Falcon Endpoint Protection Platform at a rate of 94%. Crowdstrike Falcon Endpoint Protection Platform is also in the Endpoint Protection Suites, ServiceNow Store Apps, Endpoint Management, Antivirus, Threat Intelligence, Endpoint Protection Platforms, Endpoint Detection & Response (EDR), User and Entity Behavior Analytics (UEBA), Identity Threat Detection and Response (ITDR) , AWS Marketplace, and Managed Detection and Response (MDR) categories.

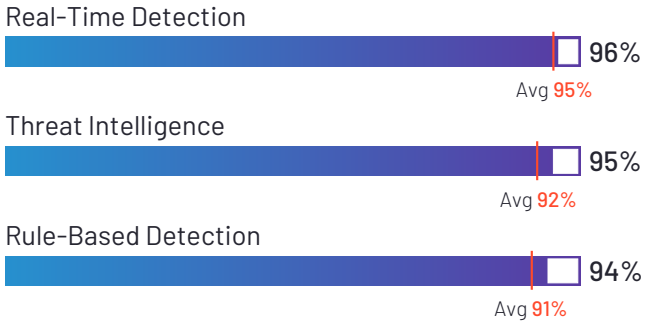
Satisfaction Ratings



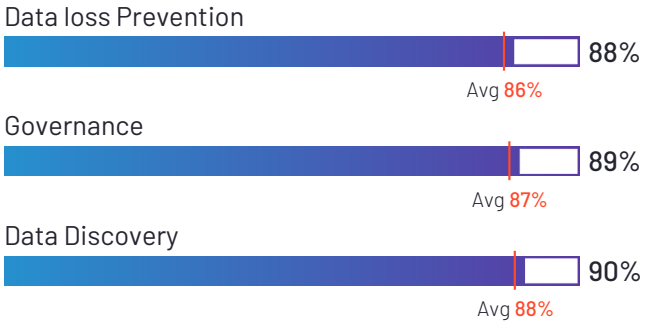
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
CrowdStrike

HQ Location
Sunnyvale, CA

Year Founded
2011

Employees (Listed On Linkedin)
6,018

Company Website
crowdstrike.com

IBM Security

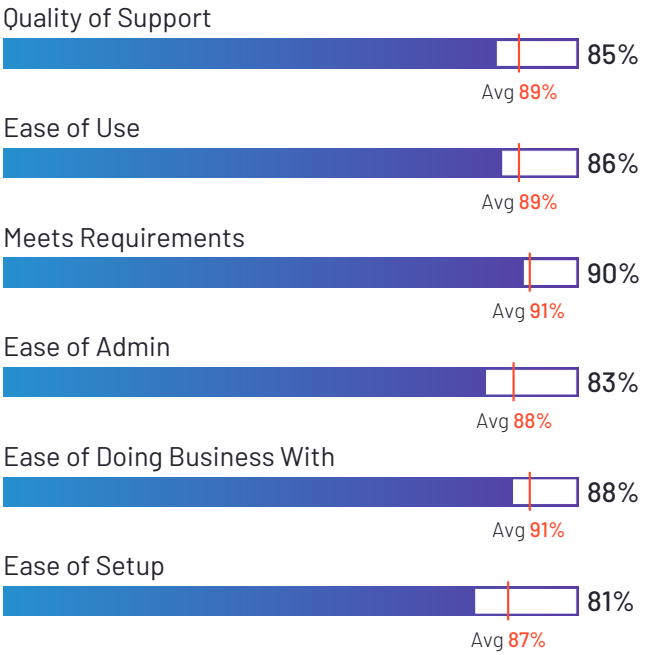
IBM Security QRadar

4.4 ★★★★½ (352)

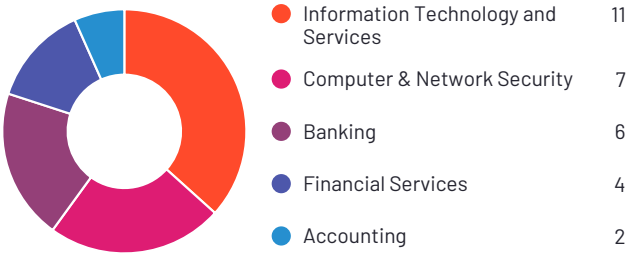
Leader FALL 2022

IBM Security QRadar has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 96% of users rated it 4 or 5 stars, 92% of users believe it is headed in the right direction, and users said they would be likely to recommend IBM Security QRadar at a rate of 90%. IBM Security QRadar is also in the Cloud Security Monitoring and Analytics, User and Entity Behavior Analytics (UEBA), Security Orchestration, Automation, and Response (SOAR), Digital Forensics, Network Traffic Analysis (NTA), Incident Response, and Security Information and Event Management (SIEM) categories.

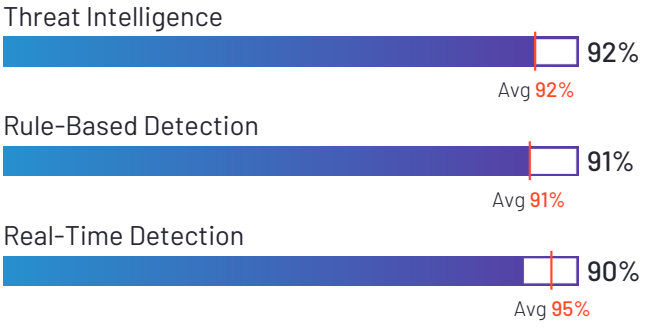
Satisfaction Ratings



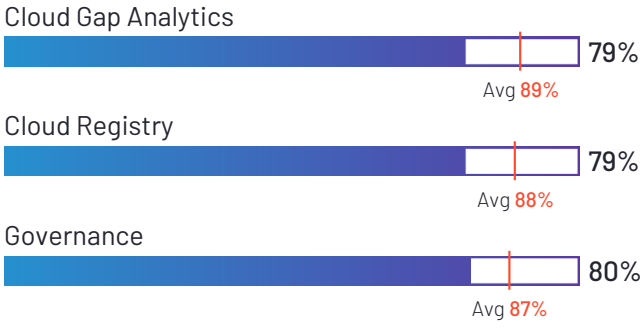
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
IBM

HQ Location
Armonk, NY

Year Founded
1911

Total Revenue
$73,621 (USD MM)

Employees (Listed On Linkedin)
531,710

Company Website
www.ibm.com

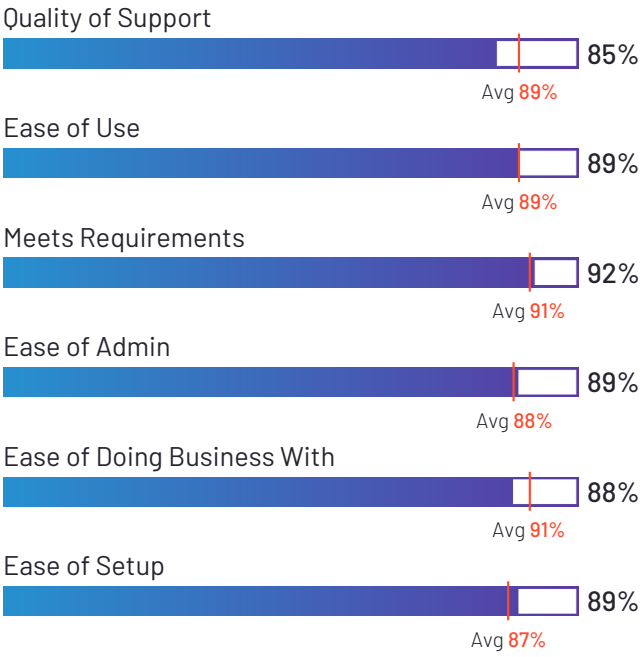
Sophos Intercept X: Next-Gen Endpoint

4.4 ★★★★½ (209)

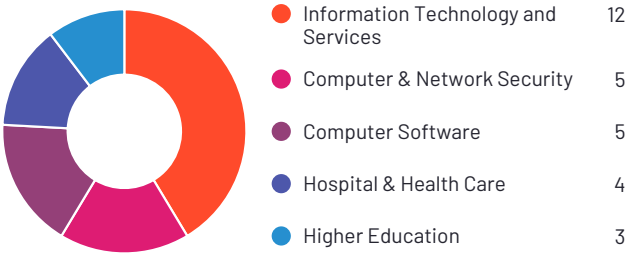
Leader FALL 2022

Sophos Intercept X: Next-Gen Endpoint has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 95% 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 Sophos Intercept X: Next-Gen Endpoint at a rate of 90%. Sophos Intercept X: Next-Gen Endpoint is also in the Endpoint Protection Suites, Antivirus, Endpoint Detection & Response (EDR), and Endpoint Protection Platforms categories.

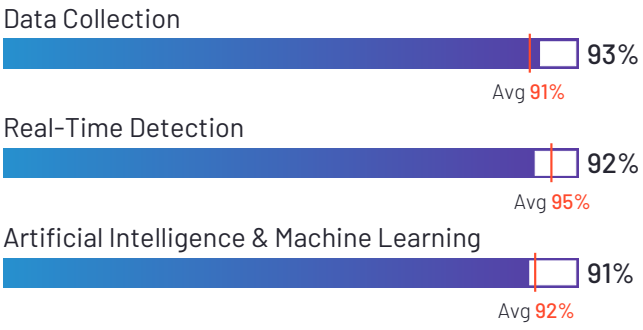
Satisfaction Ratings



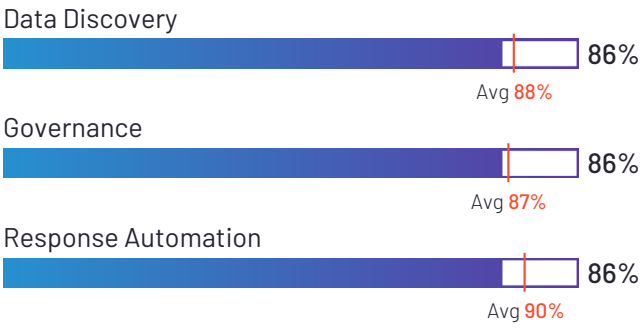
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Sophos

HQ Location
Oxfordshire, United Kingdom

Year Founded
1985

Employees (Listed On Linkedin)
4,639

Company Website
www.sophos.com

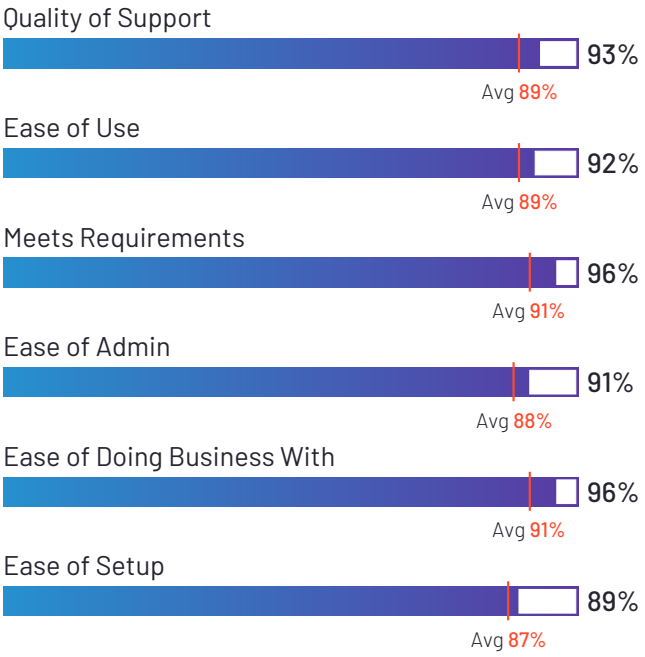
SentinelOne Singularity

4.7 ★★★★½ (65)

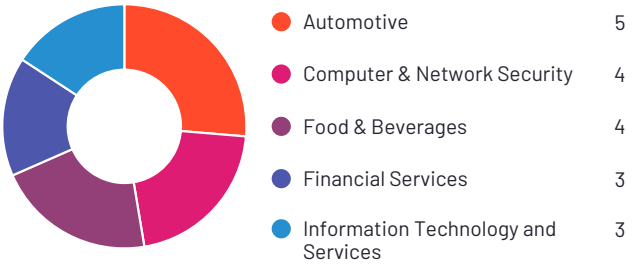
Leader FALL 2022

SentinelOne Singularity has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. 98% 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 SentinelOne at a rate of 97%. SentinelOne is also in the Endpoint Protection Suites, Antivirus, Endpoint Management, Endpoint Detection & Response (EDR), and Endpoint Protection Platforms categories.

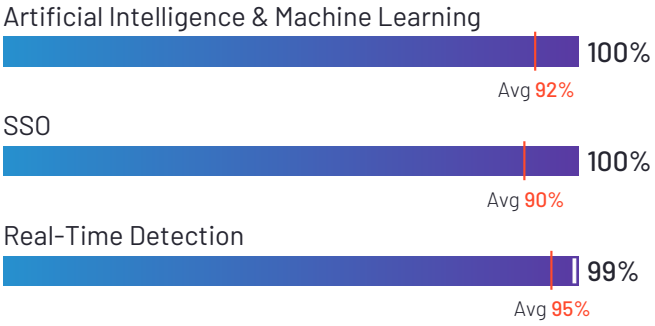
Satisfaction Ratings



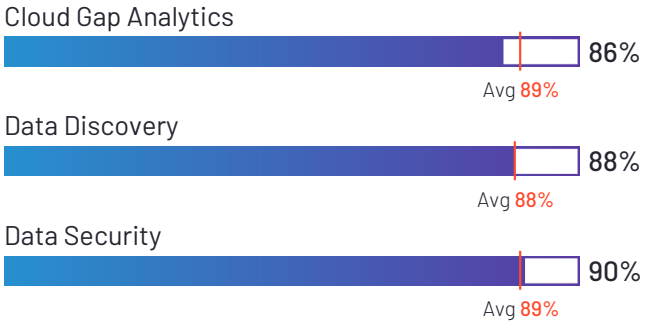
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
SentinelOne

HQ Location
Mountain View, CA

Year Founded
2013

Employees (Listed On Linkedin)
1,683

Company Website
sentinelone.com

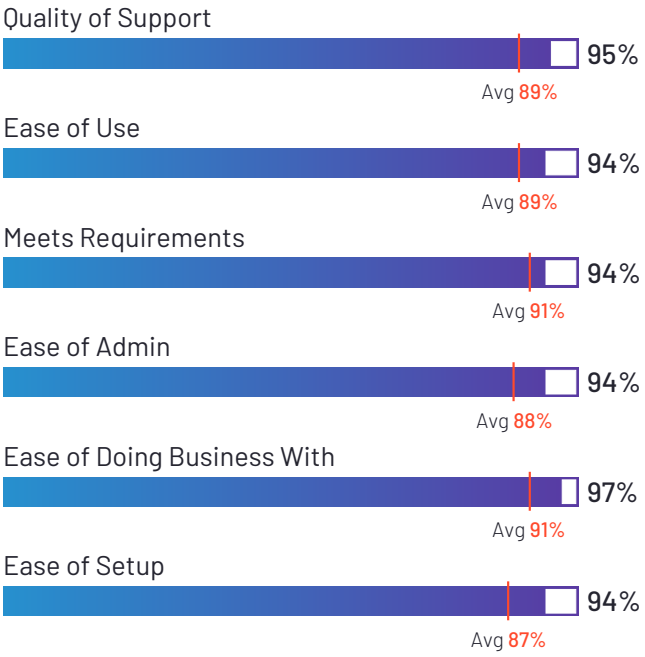
Cynet 360 AutoXDR™

4.7 ★★★★½ (130)

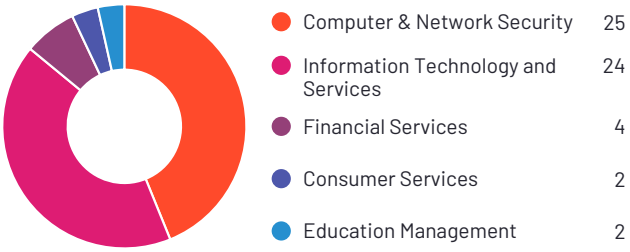
Leader FALL 2022

Cynet 360 AutoXDR™ has been named a Leader based on receiving a high customer Satisfaction score and having a large Market Presence. Cynet 360 AutoXDR™ received the highest Satisfaction score among products in Extended Detection and Response (XDR) Platforms. 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 360 AutoXDR™ at a rate of 95%. Cynet 360 AutoXDR™ is also in the Deception Technology, Endpoint Protection Platforms, User and Entity Behavior Analytics (UEBA), Endpoint Protection Suites, Endpoint Management, Endpoint Detection & Response (EDR), Incident Response, and Managed Detection and Response (MDR) categories.

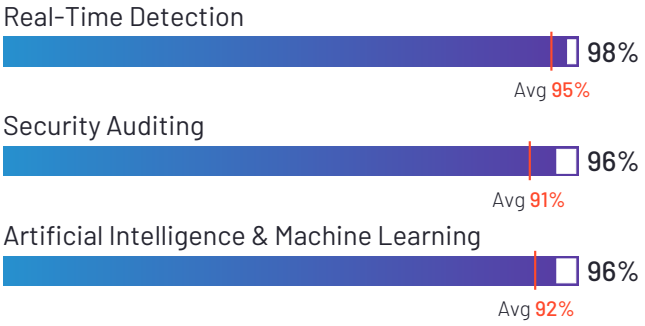
Satisfaction Ratings



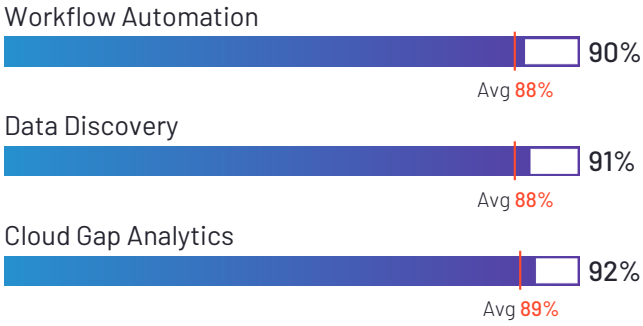
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Cynet

HQ Location
Boston, MA

Year Founded
2014

Employees (Listed On Linkedin)
279

Company Website
www.cynet.com

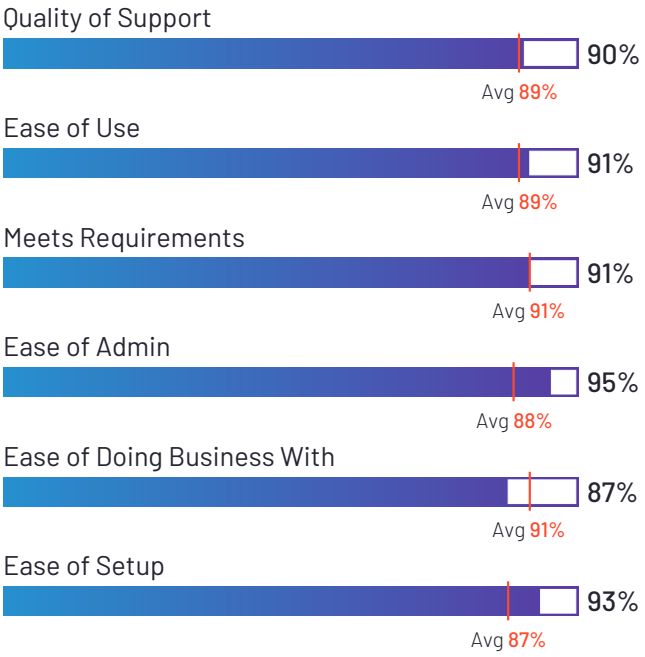
InsightIDR

4.4 ★★★★½ (62)

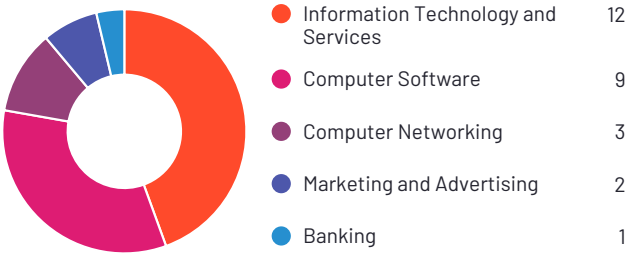
Leader FALL 2022

InsightIDR 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, 93% of users believe it is headed in the right direction, and users said they would be likely to recommend InsightIDR at a rate of 90%. InsightIDR is also in the Network Detection and Response (NDR), User and Entity Behavior Analytics (UEBA), Network Traffic Analysis (NTA), Incident Response, and Security Information and Event Management (SIEM) categories.

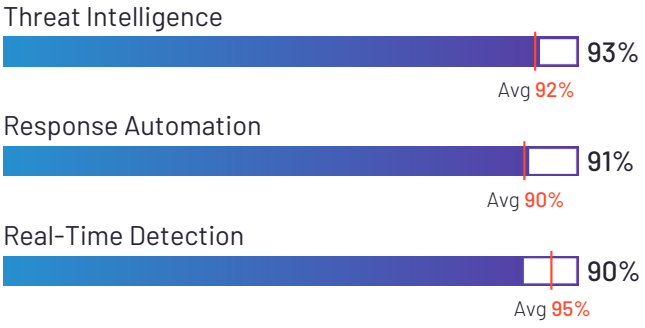
Satisfaction Ratings



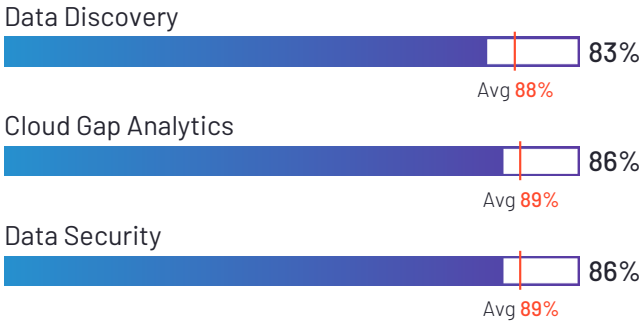
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Rapid7

HQ Location
Boston, MA

Total Revenue
$411 (USD MM)

Employees (Listed On Linkedin)
2,972

Company Website
www.rapid7.com

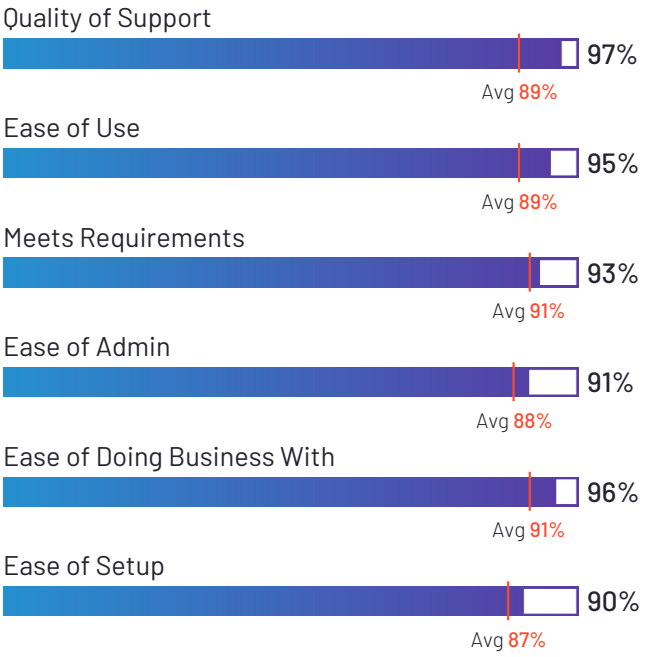
Cortex XDR

4.7 ★★★★½ (39)

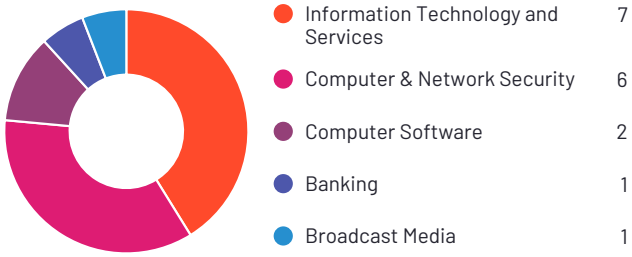
High Performer FALL 2022

Cortex XDR has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 97% of users rated it 4 or 5 stars, 95% of users believe it is headed in the right direction, and users said they would be likely to recommend Cortex XDR at a rate of 94%. Cortex XDR is also in the Network Detection and Response (NDR), Endpoint Protection Suites, Endpoint Management, Endpoint Detection & Response (EDR), and Endpoint Protection Platforms categories.

Satisfaction Ratings



Top Industries Represented



Ownership
Palo Alto Networks

HQ Location
Santa Clara, CA

Year Founded
2005

Total Revenue
$3,408 (USD MM)

Employees (Listed On Linkedin)
13,509

Company Website
paloaltonetworks.com

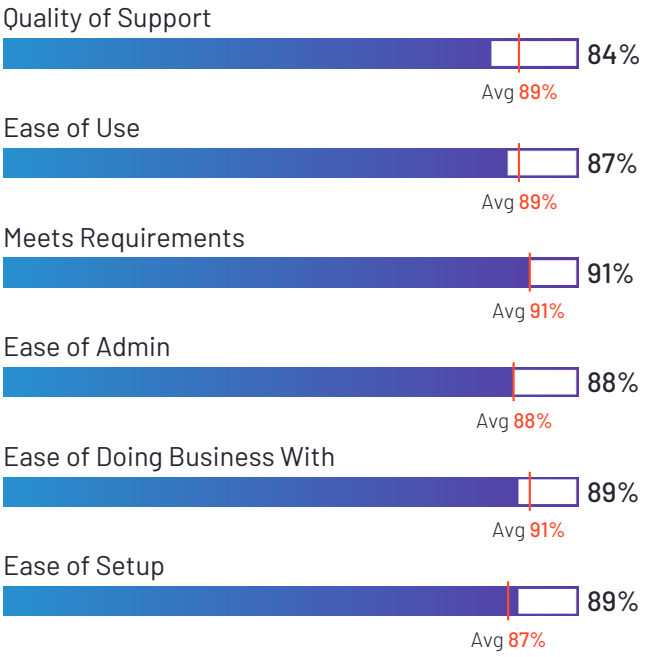
Trend Micro Apex One

4.3 ★★★★½ (92)

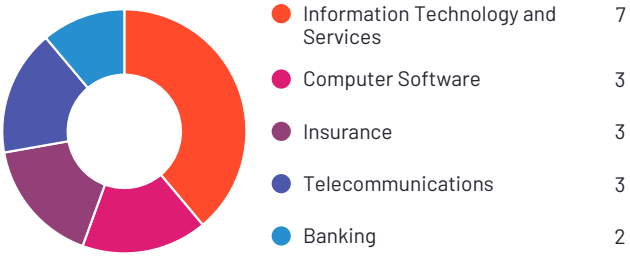
High Performer FALL 2022

Trend Micro Apex One has been named a High Performer product based on having high customer Satisfaction scores and a low Market Presence compared to the rest of the category. 92% of users rated it 4 or 5 stars, 87% of users believe it is headed in the right direction, and users said they would be likely to recommend Trend Micro at a rate of 86%. Trend Micro is also in the Endpoint Protection Suites category.

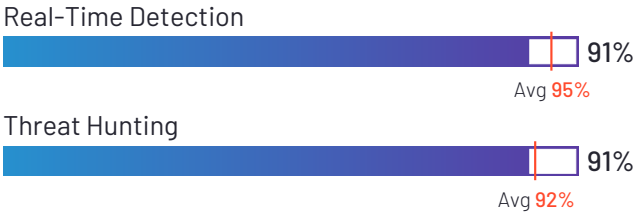
Satisfaction Ratings



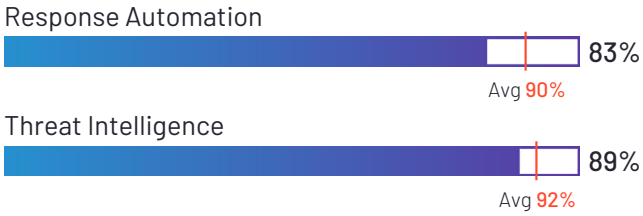
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Trend Micro

HQ Location
Tokyo, Japan

Year Founded
1988

Total Revenue
$1,515 (USD MM)

Employees (Listed On Linkedin)
7,355

Company Website
trendmicro.com

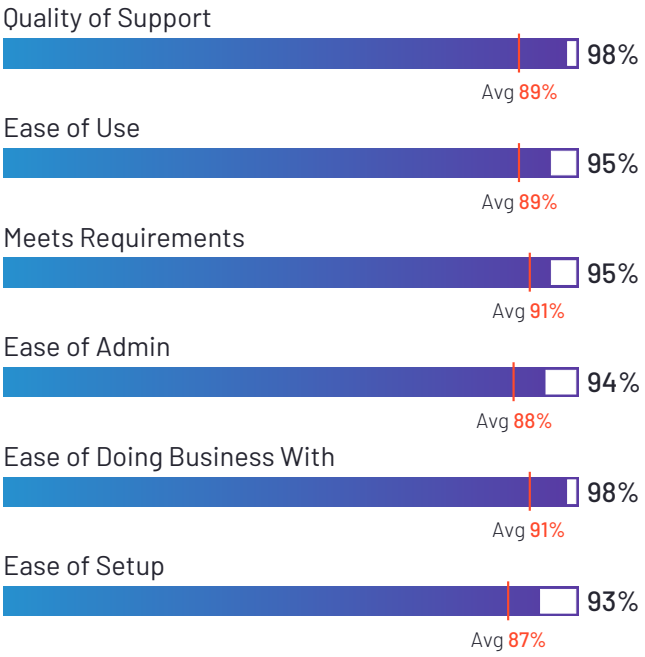
Wiz

4.9 ★★★★★ (14)

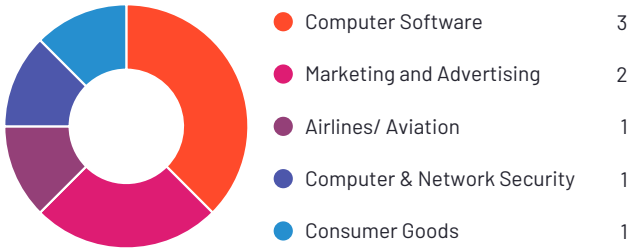
High Performer FALL 2022

Wiz 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 Wiz at a rate of 99%. Wiz is also in the Attack Surface Management, Cloud Security Posture Management (CSPM), Software Composition Analysis, Cloud Compliance, Container Security, Cloud Workload Protection Platforms, Vulnerability Scanner, Cloud Security Monitoring and Analytics, and Container Monitoring categories.

Satisfaction Ratings



Top Industries Represented



Highest-Rated Features

Lowest-Rated Features

Not enough data to include lowest-rated features for Wiz

Ownership
Wiz

HQ Location
New York, NY

Employees (Listed On Linkedin)
514

Company Website
www.wiz.io

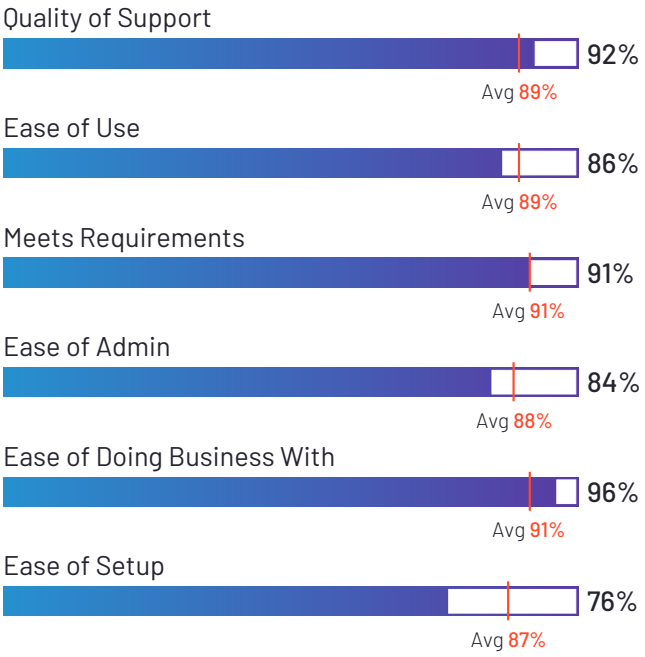
ExtraHop

4.6 ★★★★½ (52)

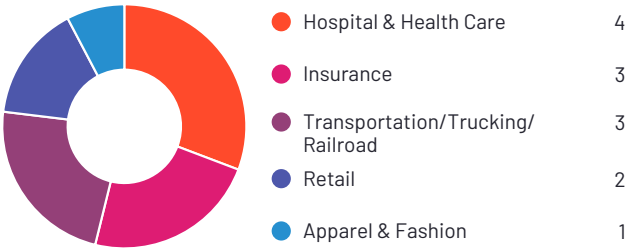
High Performer FALL 2022

ExtraHop 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, 85% of users believe it is headed in the right direction, and users said they would be likely to recommend ExtraHop at a rate of 92%. ExtraHop is also in the Network Detection and Response (NDR), Network Traffic Analysis (NTA), Intrusion Detection and Prevention Systems (IDPS), Container Security, Cloud Workload Protection Platforms, and Digital Forensics categories.

Satisfaction Ratings



Top Industries Represented



Ownership
ExtraHop Networks

HQ Location
Seattle, Washington

Year Founded
2007

Employees (Listed On Linkedin)
690

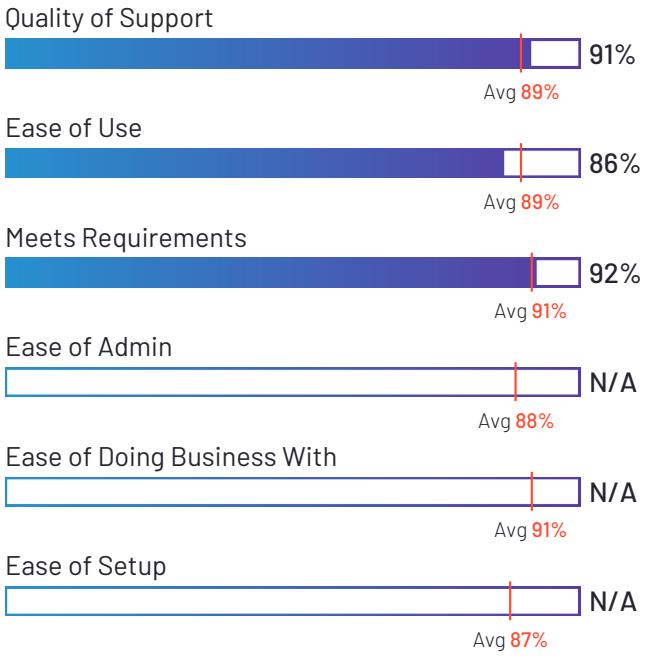
Company Website
extrahop.com

Microsoft 365 Defender

4.5 ★★★★½ (18)

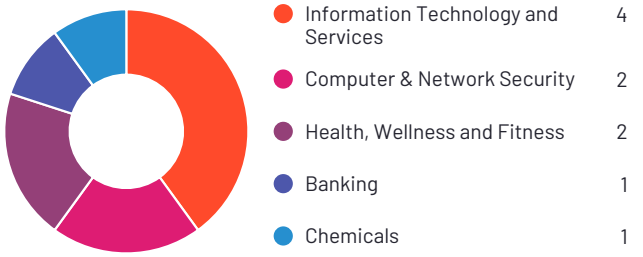
Microsoft 365 Defender has been named a Contender product based on having a relatively low customer Satisfaction score and large Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 100% of users rated it 4 or 5 stars, 100% of users believe it is headed in the right direction, and users said they would be likely to recommend Microsoft 365 Defender at a rate of 91%. Microsoft 365 Defender is also in the Cloud File Security and Cloud Email Security categories.

Satisfaction Ratings

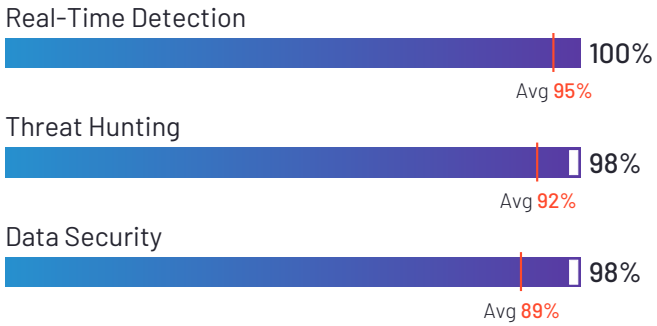


*N/A is displayed when fewer than five responses were received for the question.

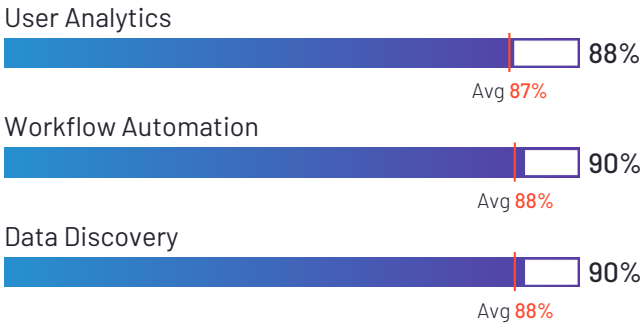
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Microsoft

HQ Location
Redmond, WA

Year Founded
1975

Total Revenue
$143,015 (USD MM)

Employees (Listed On Linkedin)
223,768

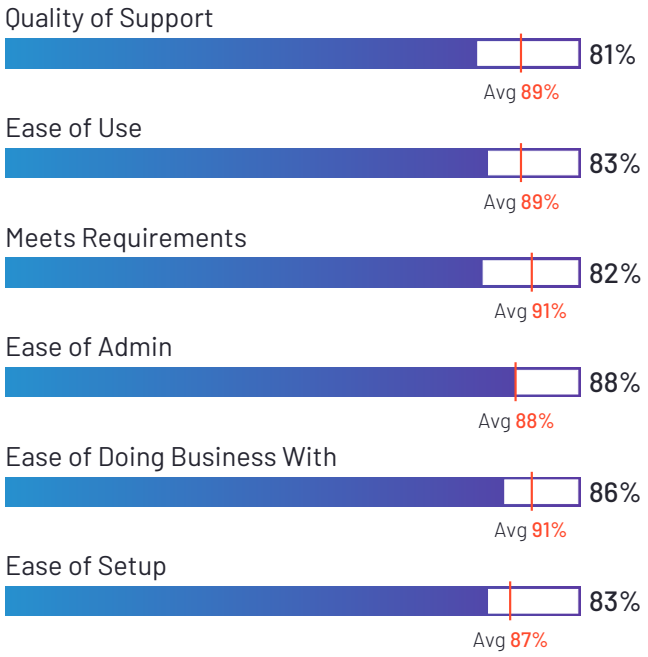
Company Website
microsoft.com

Microsoft Threat Protection

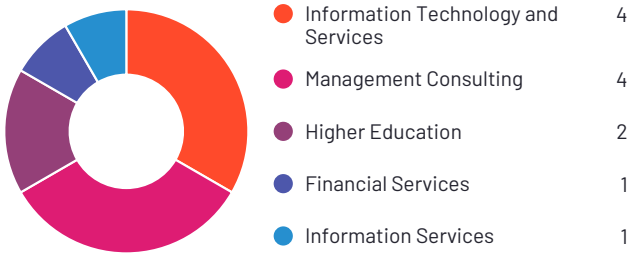
4.3 ★★★★½ (16)

Microsoft Threat Protection 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, 83% of users believe it is headed in the right direction, and users said they would be likely to recommend Microsoft Threat Protection at a rate of 86%.

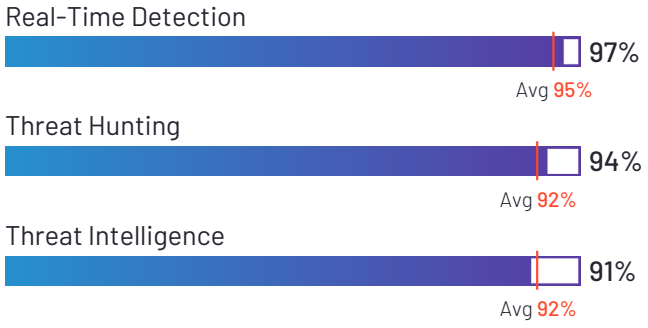
Satisfaction Ratings



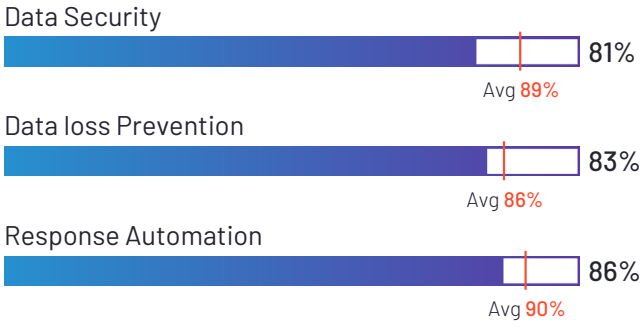
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Microsoft

HQ Location
Redmond, WA

Year Founded
1975

Total Revenue
$143,015 (USD MM)

Employees (Listed On Linkedin)
223,768

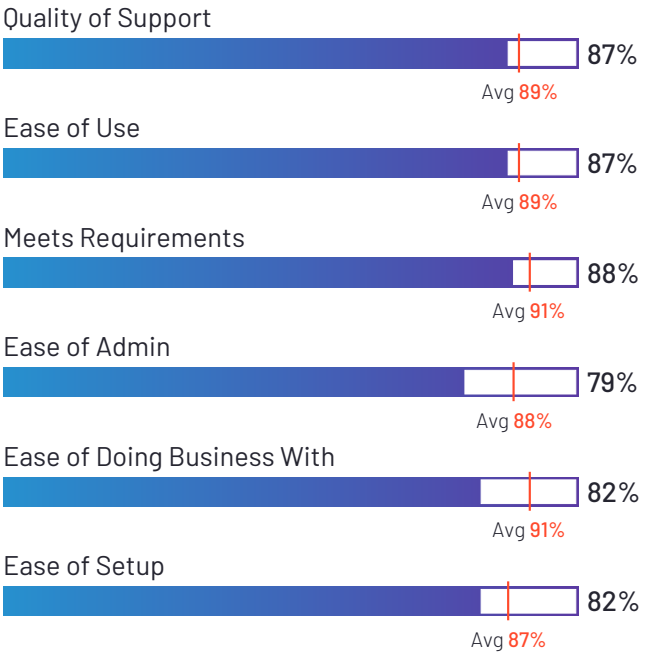
Company Website
microsoft.com

Bitdefender GravityZone

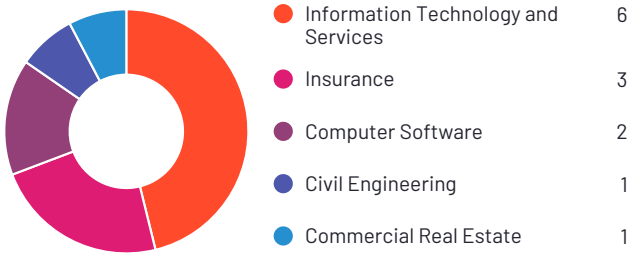
3.9 ★★★★☆ (45)

Bitdefender GravityZone 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. 81% 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 Bitdefender GravityZone at a rate of 82%. Bitdefender GravityZone is also in the Endpoint Management, Antivirus, Endpoint Detection & Response (EDR), Endpoint Protection Suites, and Endpoint Protection Platforms categories.

Satisfaction Ratings



Top Industries Represented



Ownership
Bitdefender

HQ Location
Bucuresti, Romania

Year Founded
2001

Employees (Listed On Linkedin)
2,015

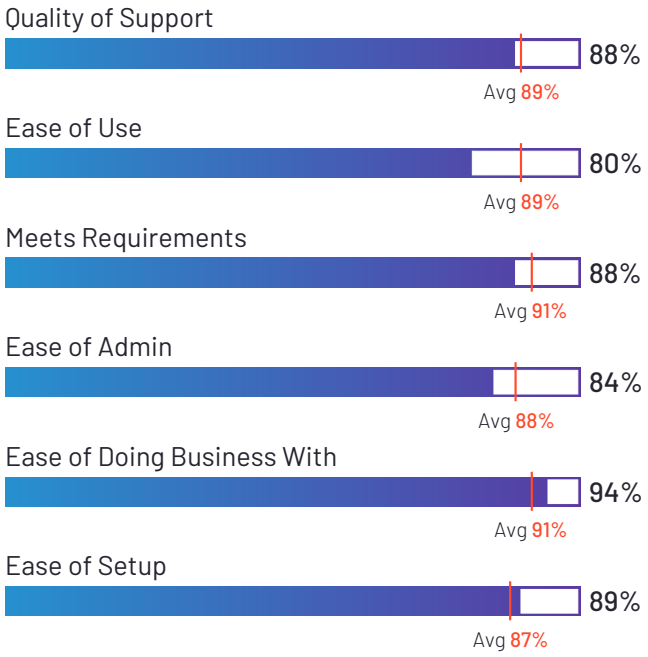
Company Website
bitdefender.com

Trend Micro Vision One (XDR)

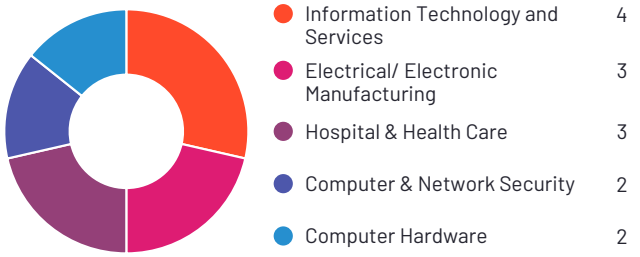
4.6 ★★★★½ (24)

Trend Micro Vision One (XDR) 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. 90% 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 Trend Micro Vision One (XDR) at a rate of 91%.

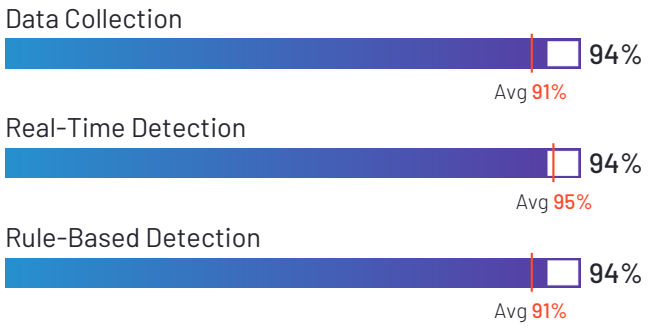
Satisfaction Ratings



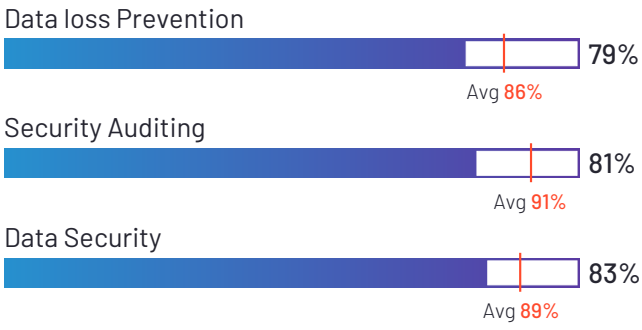
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Trend Micro

HQ Location
Tokyo, Japan

Year Founded
1988

Total Revenue
$1,515 (USD MM)

Employees (Listed On Linkedin)
7,355

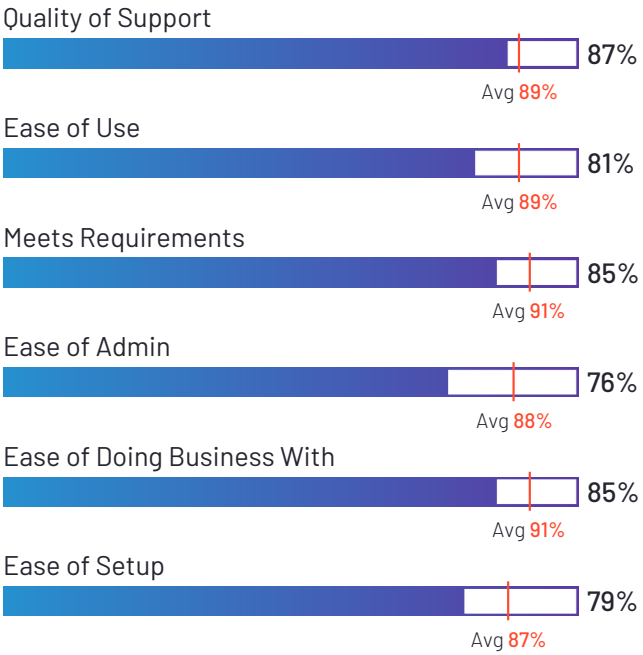
Company Website
trendmicro.com

LogRhythm NextGen SIEM Platform

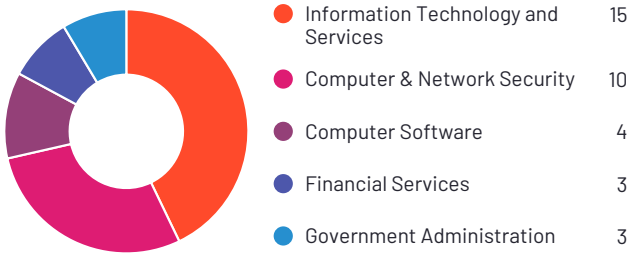
4.2 ★★★★☆ (137)

LogRhythm NextGen SIEM 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. 92% 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 LogRhythm at a rate of 80%. LogRhythm is also in the Incident Response and Security Information and Event Management (SIEM) categories.

Satisfaction Ratings



Top Industries Represented



Ownership
LogRhythm

HQ Location
Boulder, CO

Year Founded
2003

Employees (Listed On Linkedin)
615

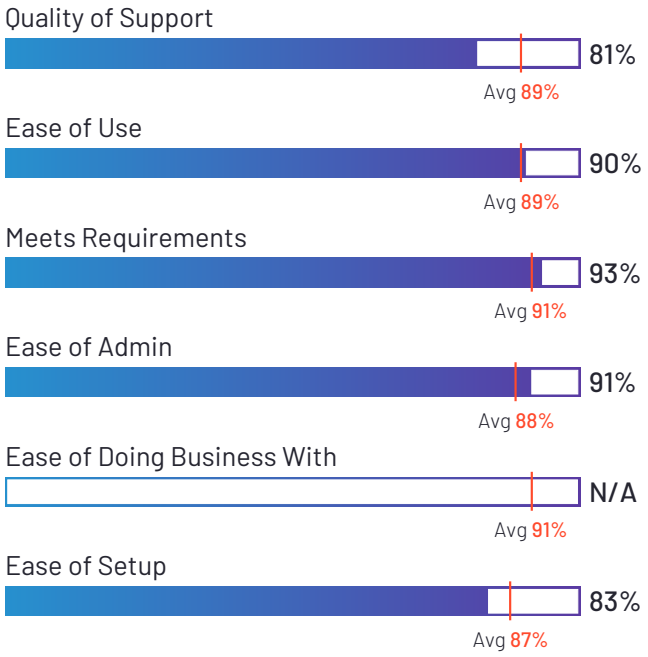
Company Website
logrhythm.com

Microsoft Defender for Cloud

4.2 ★★★★☆ (21)

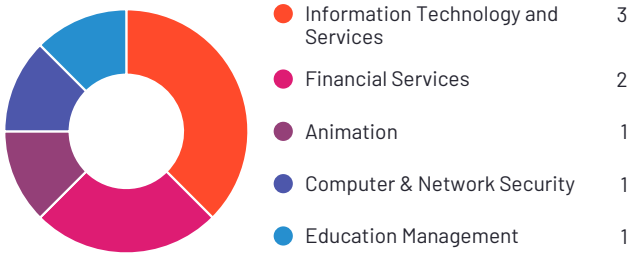
Microsoft Defender for Cloud has been named a Niche product based on having a relatively low Satisfaction score and low Market Presence compared to the rest of the category. While they may have positive reviews, they do not have enough reviews to validate those ratings. 92% of users rated it 4 or 5 stars, 90% of users believe it is headed in the right direction, and users said they would be likely to recommend Microsoft Defender for Cloud at a rate of 85%. Microsoft Defender for Cloud is also in the Cloud Compliance, Cloud Workload Protection Platforms, Security Risk Analysis, and Cloud Security Posture Management (CSPM) categories.

Satisfaction Ratings

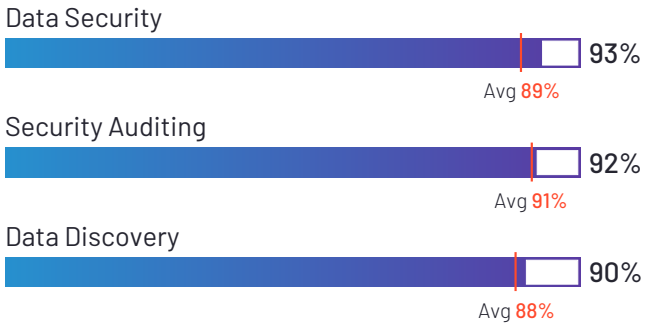


*N/A is displayed when fewer than five responses were received for the question.

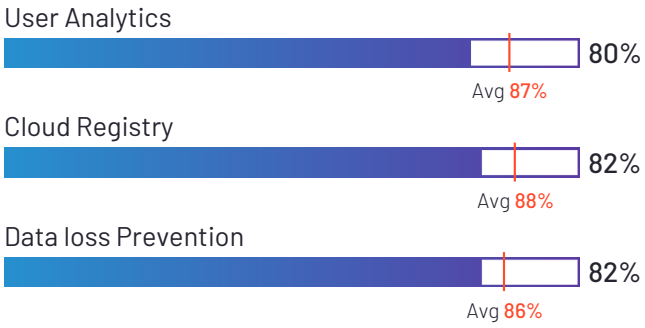
Top Industries Represented



Highest-Rated Features



Lowest-Rated Features



Ownership
Microsoft

HQ Location
Redmond, WA

Year Founded
1975

Total Revenue
$143,015 (USD MM)

Employees (Listed On Linkedin)
223,768

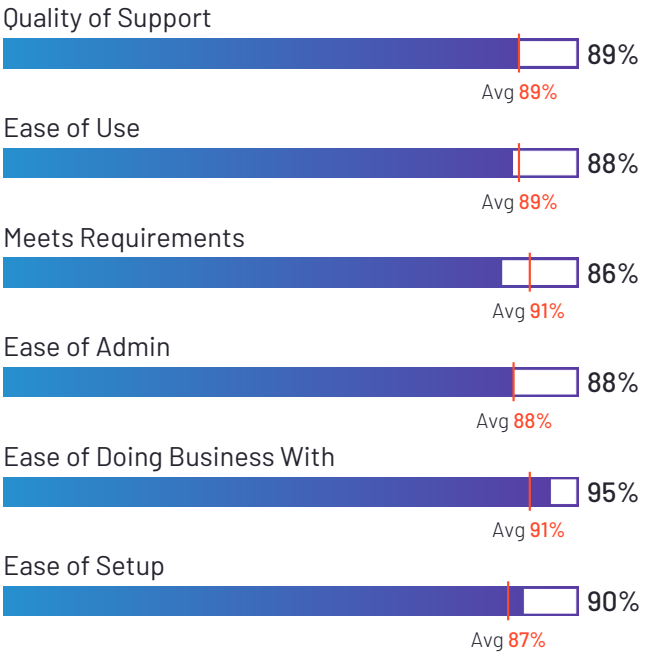
Company Website
microsoft.com

VMware Carbon Black Cloud

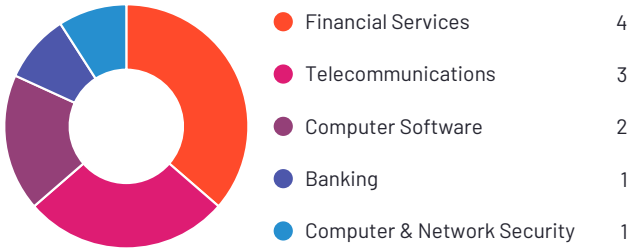
4.3 ★★★★½ (34)

VMware Carbon Black Cloud 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, 80% of users believe it is headed in the right direction, and users said they would be likely to recommend VMware Carbon Black Cloud Endpoint at a rate of 88%. VMware Carbon Black Cloud Endpoint is also in the Endpoint Protection Suites, Endpoint Management, and Antivirus categories.

Satisfaction Ratings



Top Industries Represented



Ownership
VMware

HQ Location
Palo Alto, CA

Total Revenue
$11,767 (USD MM)

Employees (Listed On Linkedin)
36,068

Company Website
www.vmware.com

Satisfaction Ratings for Extended Detection and Response (XDR) Platforms

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	Net Promoter Score (NPS) (Range from -100 to +100)
Crowdstrike Falcon Endpoint Protection Platform	94%	95%	94%	93%	93%	94%	95%	94%	87
IBM Security QRadar	90%	92%	90%	83%	88%	85%	81%	86%	68
Sophos Intercept X: Next-Gen Endpoint	90%	91%	92%	89%	88%	85%	89%	89%	70
SentinelOne	97%	97%	96%	91%	96%	93%	89%	92%	92
Cynet 360 AutoXDR™	95%	97%	94%	94%	97%	95%	94%	94%	88
InsightIDR	90%	93%	91%	95%	87%	90%	93%	91%	70
Cortex XDR	94%	95%	93%	91%	96%	97%	90%	95%	83
Trend Micro	86%	87%	91%	88%	89%	84%	89%	87%	51
Wiz	99%	100%	95%	94%	98%	98%	93%	95%	100
ExtraHop	92%	85%	91%	84%	96%	92%	76%	86%	77
Microsoft 365 Defender	91%	100%	92%	N/A	N/A	91%	N/A	86%	77
Microsoft Threat Protection	86%	83%	82%	88%	86%	81%	83%	83%	50
Bitdefender GravityZone	82%	85%	88%	79%	82%	87%	82%	87%	47
Trend Micro Vision One (XDR)	91%	92%	88%	84%	94%	88%	89%	80%	71
LogRhythm	80%	83%	85%	76%	85%	87%	79%	81%	37
Microsoft Defender for Cloud	85%	90%	93%	91%	N/A	81%	83%	90%	41
VMware Carbon Black Cloud Endpoint	88%	80%	86%	88%	95%	89%	90%	88%	54
Average	90%	91%	91%	88%	91%	89%	87%	89%	68

*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 Extended Detection and Response (XDR) Platforms

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.

Detection & Response

	Response Automation	Threat Hunting	Rule-Based Detection	Real-Time Detection
Crowdstrike Falcon Endpoint Protection Platform	93%	93%	94%	96%
IBM Security QRadar	90%	90%	91%	90%
Sophos Intercept X: Next-Gen Endpoint	86%	88%	87%	92%
SentinelOne	97%	96%	94%	99%
Cynet 360 AutoXDR™	95%	96%	93%	98%
InsightIDR	91%	86%	86%	90%
Cortex XDR	N/A	N/A	N/A	N/A
Trend Micro	83%	91%	N/A	91%
Wiz	N/A	N/A	N/A	N/A
ExtraHop	N/A	N/A	N/A	N/A
Microsoft 365 Defender	94%	98%	94%	100%
Microsoft Threat Protection	86%	94%	89%	97%
Bitdefender GravityZone	N/A	N/A	N/A	N/A
Trend Micro Vision One (XDR)	90%	93%	94%	94%
LogRhythm	N/A	N/A	N/A	N/A
Microsoft Defender for Cloud	N/A	N/A	N/A	N/A
VMware Carbon Black Cloud Endpoint	N/A	N/A	N/A	N/A
Average	90%	92%	91%	95%

(Feature Comparison for Extended Detection and Response (XDR) Platforms 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 Extended Detection and Response (XDR) Platforms (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.

Cloud Visibility

	Data Discovery	Cloud Gap Analytics
Crowdstrike Falcon Endpoint Protection Platform	90%	90%
IBM Security QRadar	81%	79%
Sophos Intercept X: Next-Gen Endpoint	86%	87%
SentinelOne	88%	86%
Cynet 360 AutoXDR™	91%	92%
InsightIDR	83%	86%
Cortex XDR	N/A	N/A
Trend Micro	N/A	N/A
Wiz		100%
ExtraHop	N/A	N/A
Microsoft 365 Defender	90%	94%
Microsoft Threat Protection	N/A	N/A
Bitdefender GravityZone	N/A	N/A
Trend Micro Vision One (XDR)	89%	N/A
LogRhythm	N/A	N/A
Microsoft Defender for Cloud	90%	89%
VMware Carbon Black Cloud Endpoint	N/A	N/A
Average	88%	89%

(Feature Comparison for Extended Detection and Response (XDR) Platforms 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 Extended Detection and Response (XDR) Platforms (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.

Security

	Security Auditing
Crowdstrike Falcon Endpoint Protection Platform	92%
IBM Security QRadar	84%
Sophos Intercept X: Next-Gen Endpoint	89%
SentinelOne	96%
Cynet 360 AutoXDR™	96%
InsightIDR	89%
Cortex XDR	N/A
Trend Micro	N/A
Wiz	100%
ExtraHop	N/A
Microsoft 365 Defender	91%
Microsoft Threat Protection	90%
Bitdefender GravityZone	N/A
Trend Micro Vision One (XDR)	81%
LogRhythm	N/A
Microsoft Defender for Cloud	92%
VMware Carbon Black Cloud Endpoint	N/A
Average	91%

(Feature Comparison for Extended Detection and Response (XDR) Platforms 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 Extended Detection and Response (XDR) Platforms (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.

Analytics

	Threat Intelligence	Data Collection
Crowdstrike Falcon Endpoint Protection Platform	95%	94%
IBM Security QRadar	92%	87%
Sophos Intercept X: Next-Gen Endpoint	87%	93%
SentinelOne	94%	96%
Cynet 360 AutoXDR™	94%	92%
InsightIDR	93%	86%
Cortex XDR	N/A	N/A
Trend Micro	89%	N/A
Wiz	N/A	N/A
ExtraHop	N/A	N/A
Microsoft 365 Defender	95%	95%
Microsoft Threat Protection	91%	86%
Bitdefender GravityZone	N/A	N/A
Trend Micro Vision One (XDR)	90%	94%
LogRhythm	N/A	N/A
Microsoft Defender for Cloud	N/A	N/A
VMware Carbon Black Cloud Endpoint	N/A	N/A
Average	92%	91%

*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 Extended Detection and Response (XDR) Platforms

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.)
Crowdstrike Falcon Endpoint Protection Platform	13%	20%	67%
IBM Security QRadar	30%	20%	50%
Sophos Intercept X: Next-Gen Endpoint	20%	66%	14%
SentinelOne	23%	28%	50%
Cynet 360 AutoXDR™	45%	46%	9%
InsightIDR	19%	62%	19%
Cortex XDR	17%	43%	40%
Trend Micro	15%	60%	26%
Wiz	9%	55%	36%
ExtraHop	5%	23%	73%
Microsoft 365 Defender	44%	33%	22%
Microsoft Threat Protection	7%	71%	21%
Bitdefender GravityZone	43%	38%	19%
Trend Micro Vision One (XDR)	30%	35%	35%
LogRhythm	13%	49%	38%
Microsoft Defender for Cloud	42%	25%	33%
VMware Carbon Black Cloud Endpoint	5%	50%	45%
Average	22%	43%	35%

(Additional Data for Extended Detection and Response (XDR) Platforms continues on next page)

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

Additional Data for Extended Detection and Response (XDR) Platforms (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)
Crowdstrike Falcon Endpoint Protection Platform	65%	35%	1.2	64%	27%	3%	6%	37	23
IBM Security QRadar	52%	48%	3.1	52%	36%	12%	0%	17	19
Sophos Intercept X: Next-Gen Endpoint	70%	30%	2.0	79%	17%	2%	2%	175	20
SentinelOne	94%	6%	1.6	74%	17%	4%	4%	750	26
Cynet 360 AutoXDR™	83%	17%	0.8	82%	14%	0%	5%	37	10
InsightIDR	86%	14%	0.8	86%	0%	14%	0%	7	12
Cortex XDR	54%	46%	1.4	57%	29%	14%	0%	750	22
Trend Micro	75%	25%	0.7	78%	6%	17%	0%	75	13
Wiz	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
ExtraHop	29%	71%	2.1	71%	14%	0%	14%	N/A	17
Microsoft 365 Defender	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Microsoft Threat Protection	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Bitdefender GravityZone	79%	21%	1.5	92%	8%	0%	0%	37	22
Trend Micro Vision One (XDR)	90%	10%	1.7	70%	30%	0%	0%	37	15
LogRhythm	25%	75%	3.1	23%	50%	15%	12%	7	20
Microsoft Defender for Cloud	100%	0%	4.0	100%	0%	0%	0%	17	N/A
VMware Carbon Black Cloud Endpoint	95%	5%	2.5	89%	11%	0%	0%	375	21

(Additional Data for Extended Detection and Response (XDR) Platforms continues on next page)

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

Additional Data for Extended Detection and Response (XDR) Platforms (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)
Crowdstrike Falcon Endpoint Protection Platform	88%	19
IBM Security QRadar	72%	17
Sophos Intercept X: Next-Gen Endpoint	83%	19
SentinelOne	93%	15
Cynet 360 AutoXDR™	79%	12
InsightIDR	79%	14
Cortex XDR	83%	N/A
Trend Micro	82%	13
Wiz	N/A	N/A
ExtraHop	70%	N/A
Microsoft 365 Defender	N/A	N/A
Microsoft Threat Protection	N/A	N/A
Bitdefender GravityZone	95%	17
Trend Micro Vision One (XDR)	71%	15
LogRhythm	57%	23
Microsoft Defender for Cloud	90%	22
VMware Carbon Black Cloud Endpoint	83%	18
Average	80%	17

(Additional Data for Extended Detection and Response (XDR) Platforms continues on next page)

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

Additional Data for Extended Detection and Response (XDR) Platforms (continued)

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

Market Presence

	Seller Name	Year Founded	Revenue ($MM)	Employees on LinkedIn (Seller)	LinkedIn Followers	Twitter Followers (Seller)	Glassdoor Rating
Crowdstrike Falcon Endpoint Protection Platform	CrowdStrike	2011	N/A	6,018	337,469	68,652	4.4
IBM Security QRadar	IBM	1911	$73,621	531,710	14,296,858	696,414	4.1
Sophos Intercept X: Next-Gen Endpoint	Sophos	1985	N/A	4,639	323,973	36,077	3.9
SentinelOne	SentinelOne	2013	N/A	1,683	104,889	18,209	4.9
Cynet 360 AutoXDR™	Cynet	2014	N/A	279	11,840	908	N/A
InsightIDR	Rapid7		$411	2,972	118,374	115,211	4.3
Cortex XDR	Palo Alto Networks	2005	$3,408	13,509	745,841	119,476	4.1
Trend Micro	Trend Micro	1988	$1,515	7,355	202,261	114,157	4.1
Wiz	Wiz		N/A	514	25,143	0	N/A
ExtraHop	ExtraHop Networks	2007	N/A	690	24,057	11,334	4.3
Microsoft 365 Defender	Microsoft	1975	$143,015	223,768	17,587,038	11,472,744	4.4
Microsoft Threat Protection	Microsoft	1975	$143,015	223,768	17,587,038	11,472,744	4.4
Bitdefender GravityZone	Bitdefender	2001	N/A	2,015	137,063	110,749	4.0
Trend Micro Vision One (XDR)	Trend Micro	1988	$1,515	7,355	202,261	114,157	4.1
LogRhythm	LogRhythm	2003	N/A	615	39,025	7,978	3.8
Microsoft Defender for Cloud	Microsoft	1975	$143,015	223,768	17,587,038	11,472,744	4.4
VMware Carbon Black Cloud Endpoint	VMware		$11,767	36,068	1,717,813	333,958	4.5

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