Endpoint Detection and Response Buyers Guide

Software Provider and Product Assessment

EXECUTIVE SUMMARY

ISG Research

Endpoint Detection and Response

Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and Information Security (InfoSec) leaders face an ever-evolving cyber threat reality. As businesses rely more on digital infrastructures, the urgency to protect sensitive data and ensure operational integrity grows. A strategic approach that blends innovation with effective management of security technologies is essential. Utilizing advanced cybersecurity software tools is crucial for countering emerging threats and fortifying defenses against diverse cyber risks. Enterprises must grasp the capabilities and intricacies of these tools to safeguard valuable assets, enhance compliance and reduce security breaches. Data breaches can inflict significant financial and reputational damage, making proactive measures and incident response protocols vital for effective defense and recovery. This Buyers Guide offers insights to help enterprise security leaders make informed decisions on selecting and deploying critical cybersecurity technologies, ultimately improving their security posture and fostering a safer digital environment.

> **ISG Research defines Endpoint Detection and Response as a modern cybersecurity strategy focused on detecting, investigating and responding to advanced threats on endpoint devices, including computers, laptops and servers.**

ISG Research defines Endpoint Detection and Response (EDR) as a modern cybersecurity strategy focused on detecting, investigating and responding to advanced threats on endpoint devices, including computers, laptops and servers. As the endpoints are often the primary attack vectors for adversaries, effective EDR approaches provide enterprises with comprehensive visibility into endpoint activity, enabling rapid detection of potential threats. EDR tools continuously monitor endpoints for suspicious behaviors and indicators of compromise (IOCs) that may signify a security breach.

By leveraging advanced analytics, machine learning (ML) and behavioral analysis, EDR approaches can differentiate between normal and anomalous activities, allowing security teams to respond in real time. Upon detection of a threat, EDR tools can automate response actions, such as isolating infected systems, terminating malicious processes or quarantining suspicious files, thus minimizing damage and reducing response times. Additionally, EDR software tools often include incident investigation capabilities, offering security teams the ability to conduct forensic analysis, understand attack vectors and identify root causes.

Beyond detection and response, EDR also emphasizes proactive threat hunting and vulnerability management, enabling enterprises to identify weaknesses before they can be exploited. Modern cyber threats are continually evolving, so integrating robust EDR capabilities is crucial for bolstering an enterprise's defenses. By focusing on endpoint security, EDR enhances overall enterprise resilience, helping to protect against sophisticated cyberattacks while ensuring business continuity. ISG asserts that by 2027, 4 in 5 enterprises will implement proactive detection and response software for endpoints and machines, enabling security technicians to prioritize threat hunting.

Cybersecurity

Market Assertion

By 2027, 4 in 5 enterprises will implement proactive detection and response software for endpoints and machines, enabling security technicians to prioritize threat hunting.

Jeff Orr
Director of Research, Technology Research

ISG Research

Adopting EDR can significantly contribute to enhancing an enterprise's security posture by focusing on detecting, analyzing and responding to threats at the endpoint level. With the proliferation of remote work and an increasing number of devices accessing corporate networks, endpoints have become prime targets for cyberattacks. EDR tools provide visibility into endpoint activities, enabling security teams to detect suspicious behaviors and potential threats in real time. This proactive monitoring is essential for early threat identification, reducing the risk of data breaches and system compromises.

An EDR approach can also streamline incident response capabilities by automating containment and remediation actions. When a threat is detected, EDR can autonomously respond, isolating compromised devices to prevent lateral movement within the network. This rapid response capability not only mitigates threats quickly but also minimizes downtime, which is critical for maintaining business operations and productivity.

Additionally, EDR approaches often incorporate threat intelligence and analytics, empowering security teams to hunt for hidden threats before they can exploit vulnerabilities. By enhancing overall endpoint security, EDR supports enterprise goals such as operational resilience, regulatory compliance and customer trust. In an environment where cyber threats are increasingly sophisticated, a robust EDR strategy is indispensable for enterprises looking to strengthen their cybersecurity posture while achieving their business objectives.

Generative AI (GenAI) is transforming enterprise cybersecurity software by automating complex processes and enhancing decision-making. By leveraging GenAI, enterprises can streamline threat detection, optimize resource allocation and proactively identify vulnerabilities, leading to improved operational performance. Additionally, GenAI enables teams to extract valuable insights from extensive data, fostering informed strategic planning and collaboration. As enterprises navigate digital transformation, integrating cybersecurity software with GenAI capabilities becomes crucial for maintaining a competitive edge and enhancing organizational resilience.

GenAI is already making significant strides within EDR software, enhancing various enterprise applications. For instance, it elevates threat hunting by automating the analysis of endpoint telemetry and prioritizing alerts based on risk, allowing security teams to focus on the most pertinent issues. This AI-driven approach empowers security professionals to identify vulnerabilities and suspicious activities proactively, fostering a more preemptive security stance. In addition, during incident response, GenAI tools can recommend immediate containment actions and efficiently synchronize responses across multiple endpoints, ultimately streamlining the process and improving the quality of post-incident reviews. The combination of these capabilities not only increases productivity but also enhances the overall effectiveness of security personnel in managing endpoint threats.

Looking toward the future, the integration of Agentic AI functionalities into EDR software promises transformative changes for enterprise security management. With this capability, Agentic AI could take on the role of an autonomous guardian, consistently monitoring endpoints for signs of compromise while making real-time decisions about threat response without human intervention. For example, it might isolate infected devices instantly, implement remediation tactics and conduct system rollbacks to restore safe operating conditions, all while learning from ongoing incidents to fine-tune its detection and reaction strategies. This approach would improve the agility of EDR systems, allowing security teams to redirect their focus toward more strategic initiatives, confident that intelligent systems are effectively managing immediate threats. As a result, enterprises could achieve a greatly enhanced security posture, better equipped to handle the evolving landscape of cyber threats.

> “**CIOs and security leaders should approach cybersecurity software incorporating GenAI, large language models and future agentic AI capabilities with enthusiasm and caution.**

CIOs and security leaders should approach cybersecurity software incorporating GenAI, large language models (LLMs) and future agentic AI capabilities with enthusiasm and caution. While these technologies offer significant benefits, they also come with unique challenges and prerequisites. A holistic evaluation must include technical aspects and business, ethical and strategic considerations. Other areas of focus include risk awareness, critical infrastructure, organizational readiness, governance and compliance, and a long-term perspective on the sustainability and scalability of AI approaches.

Our Cybersecurity Buyers Guide research is designed to provide a comprehensive view of a software provider’s capability to enhance the effectiveness, performance and governance of cybersecurity measures within an enterprise. Separate Buyers Guide research reports are available for SIEM, IAM and Data Recovery software.

ISG believes a methodical approach is essential to maximize competitiveness. It is critical to select the right software provider and product to improve the performance of your enterprise's people, process, information and technology components.

The insights gained from understanding current cybersecurity software providers are invaluable for enterprise CIOs, CISOs and VPs of InfoSec who aim to align their technology investments with organizational goals, enhance security workflows and cultivate a culture of resilience. By investing in the right cybersecurity tools, these leaders can unlock new avenues for protection and transformation, positioning their enterprises to thrive.

The ISG Buyers Guide™ for EDR evaluates products based on a variety of capabilities, including the use of GenAI and machine learning, automated response, incident forensics, integration with other tools, threat detection, threat hunting and the ability for an enterprise to migrate to an MSP relationship with the product later. To be included in this Buyers Guide, software providers must meet or exceed the inclusion criteria and have commercially available products marketed for large enterprise licensing.

This research evaluates the following software providers that offer products addressing key elements of EDR: Acronis, Arctic Wolf, Bitdefender, Broadcom, Check Point, Cisco, CrowdStrike, Cybereason, ESET, Fortinet, ManageEngine, Microsoft, Palo Alto Networks, Qualys, SentinelOne, Sophos, Trellix, Trend Micro and WithSecure.

Buyers Guide Overview

For over two decades, ISG Research has conducted market research in a spectrum of areas across business applications, tools and technologies. We have designed the Buyers Guide to provide a balanced perspective of software providers and products that is rooted in an understanding of the business requirements in any enterprise. Utilization of our research methodology and decades of experience enables our Buyers Guide to be an effective method to assess and select software providers and products. The findings of this research undertaking contribute to our comprehensive approach to rating software providers in a manner that is based on the assessments completed by an enterprise.

> **ISG Research has designed the Buyers Guide to provide a balanced perspective of software providers and products that is rooted in an understanding of business requirements in any enterprise.**

The ISG Buyers Guide™ for Endpoint Detection and Response is the distillation of over a year of market and product research efforts. It is an assessment of how well software providers' offerings address enterprises' requirements for EDR software. The index is structured to support a request for information (RFI) that could be used in the request for proposal (RFP) process by incorporating all criteria needed to evaluate, select, utilize and maintain relationships with software providers. An effective product and customer experience with a provider can ensure the best long-term relationship and value achieved from a resource and financial investment.

In this Buyers Guide, ISG Research evaluates the software in seven key categories that are weighted to reflect buyers' needs based on our expertise and research. Five are product-experience related: Adaptability, Capability, Manageability, Reliability, and Usability. In addition, we consider two customer-experience categories: Validation, and Total Cost of Ownership/Return on Investment (TCO/ROI). To assess functionality, one of the components of Capability, we applied the ISG Research Value Index methodology and blueprint, which links the personas and processes for EDR to an enterprise's requirements.

The structure of the research reflects our understanding that the effective evaluation of software providers and products involves far more than just examining product features, potential revenue or customers generated from a provider's marketing and sales efforts. We believe it is important to take a comprehensive, research-based approach, since making the wrong choice of EDR technology can raise the total cost of ownership, lower the return on investment and hamper an enterprise's ability to reach its full performance potential. In addition, this approach can reduce the project's development and deployment time and eliminate the risk of relying on a short list of software providers that does not represent a best fit for your enterprise.

ISG Research believes that an objective review of software providers and products is a critical business strategy for the adoption and implementation of EDR software and applications. An enterprise's review should include a thorough analysis of both what is possible and what is relevant. We urge enterprises to do a thorough job of evaluating EDR systems and tools and offer this Buyers Guide as both the results of our in-depth analysis of these providers and as an evaluation methodology.

How To Use This Buyers Guide

Evaluating Software Providers: The Process

We recommend using the Buyers Guide to assess and evaluate new or existing software providers for your enterprise. The market research can be used as an evaluation framework to establish a formal request for information from providers on products and customer experience and will shorten the cycle time when creating an RFI. The steps listed below provide a process that can facilitate best possible outcomes.

1. Define the business case and goals.

   Define the mission and business case for investment and the expected outcomes from your organizational and technological efforts.
2. Specify the business needs.

   Defining the business requirements helps identify what specific capabilities are required with respect to people, processes, information and technology.
3. Assess the required roles and responsibilities.

   Identify the individuals required for success at every level of the enterprise from executives to frontline workers and determine the needs of each.
4. Outline the project's critical path.

   What needs to be done, in what order and who will do it? This outline should make clear the prior dependencies at each step of the project plan.
5. Ascertain the technology approach.

   Determine the business and technology approach that most closely aligns to your enterprise's requirements.
6. Establish software provider evaluation criteria.

   Utilize the product experience: Adaptability, Capability, Manageability, Reliability and Usability, and the customer experience in TCO/ROI and Validation.
7. Evaluate and select the technology properly.

   Weight the categories in the technology evaluation criteria to reflect your enterprise's priorities to determine the short list of software providers and products.
8. Establish the business initiative team to start the project.

   Identify who will lead the project and the members of the team needed to plan and execute it with timelines, priorities and resources.

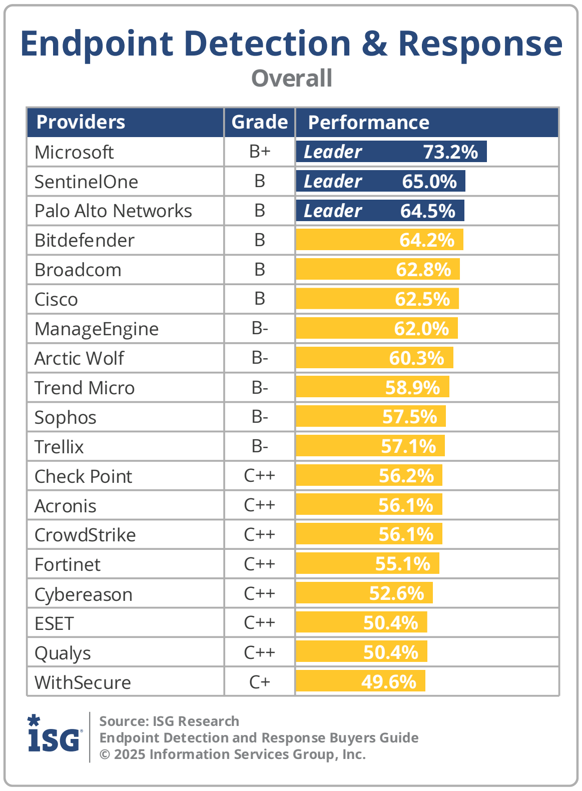
The Findings

All of the products we evaluated are feature-rich, but not all the capabilities offered by a software provider are equally valuable to types of workers or support everything needed to manage products on a continuous basis. Moreover, the existence of too many capabilities may be a negative factor for an enterprise if it introduces unnecessary complexity. Nonetheless, you may decide that a larger number of features in the product is a plus, especially if some of them match your enterprise's established practices or support an initiative that is driving the purchase of new software.

Factors beyond features and functions or software provider assessments may become a deciding factor. For example, an enterprise may face budget constraints such that the TCO evaluation can tip the balance to one provider or another. This is where the Value Index methodology and the appropriate category weighting can be applied to determine the best fit of software providers and products to your specific needs.

Overall Scoring of Software Providers Across Categories

The research finds Microsoft atop the list, followed by SentinelOne and Palo Alto Networks. Providers that place in the top three of a category earn the designation of Leader. Microsoft has done so in seven categories; Broadcom in five; ManageEngine in four; and Bitdefender, CrowdStrike, Fortinet, Palo Alto Networks and SentinelOne in one category.



Endpoint Detection & Response

Overall

Providers	Grade	Performance
Microsoft	B+	Leader 73.2%
SentinelOne	B	Leader 65.0%
Palo Alto Networks	B	Leader 64.5%
Bitdefender	B	64.2%
Broadcom	B	62.8%
Cisco	B	62.5%
ManageEngine	B-	62.0%
Arctic Wolf	B-	60.3%
Trend Micro	B-	58.9%
Sophos	B-	57.5%
Trellix	B-	57.1%
Check Point	C++	56.2%
Acronis	C++	56.1%
CrowdStrike	C++	56.1%
Fortinet	C++	55.1%
Cybereason	C++	52.6%
ESET	C++	50.4%
Qualys	C++	50.4%
WithSecure	C+	49.6%

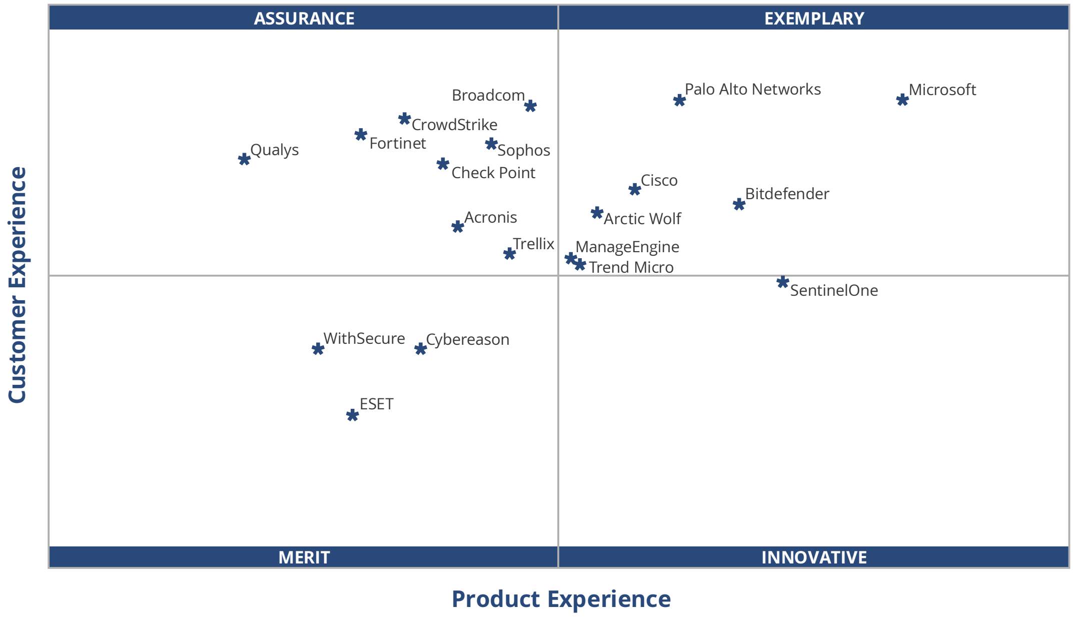
Source: ISG Research
Endpoint Detection and Response Buyers Guide
© 2025 Information Services Group, Inc.

The overall representation of the research below places the rating of the Product Experience and Customer Experience on the *x* and *y* axes, respectively, to provide a visual representation and classification of the software providers. Those providers whose Product Experience have a higher weighted performance to the axis in aggregate of the five product categories place farther to the right, while the performance and weighting for the two Customer Experience categories determines placement on the vertical axis. In short, software providers that place closer to the upper-right on this chart performed better than those closer to the lower-left.

The research places software providers into one of four overall categories: Assurance, Exemplary, Merit or Innovative. This representation classifies providers' overall weighted performance.

Endpoint Detection and Response

ISG Buyers Guide™



Source: ISG Research
Endpoint Detection and Response Buyers Guide
© 2025 Information Services Group, Inc.

Exemplary: The categorization and placement of software providers in Exemplary (upper right) represent those that performed the best in meeting the overall Product and Customer Experience requirements. The providers rated Exemplary are: Arctic Wolf, Bitdefender, Cisco, ManageEngine, Microsoft, Palo Alto Networks and Trend Micro.

Innovative: The categorization and placement of software providers in Innovative (lower right) represent those that performed the best in meeting the overall Product Experience requirements but did not achieve the highest levels of requirements in Customer Experience. The provider rated Innovative is: SentinelOne.

Assurance: The categorization and placement of software providers in Assurance (upper left) represent those that achieved the highest levels in the overall Customer Experience requirements but did not achieve the highest levels of Product Experience. The providers rated Assurance are: Acronis, Broadcom, Check Point, CrowdStrike, Fortinet, Qualys, Sophos and Trellix.

Merit: The categorization of software providers in Merit (lower left) represents those that did not reach the rating of Assurance, Exemplary or Innovative ratings in Customer or Product Experience or surpass the threshold for the other three categories. The providers rated Merit are: Cybereason, ESET and WithSecure.

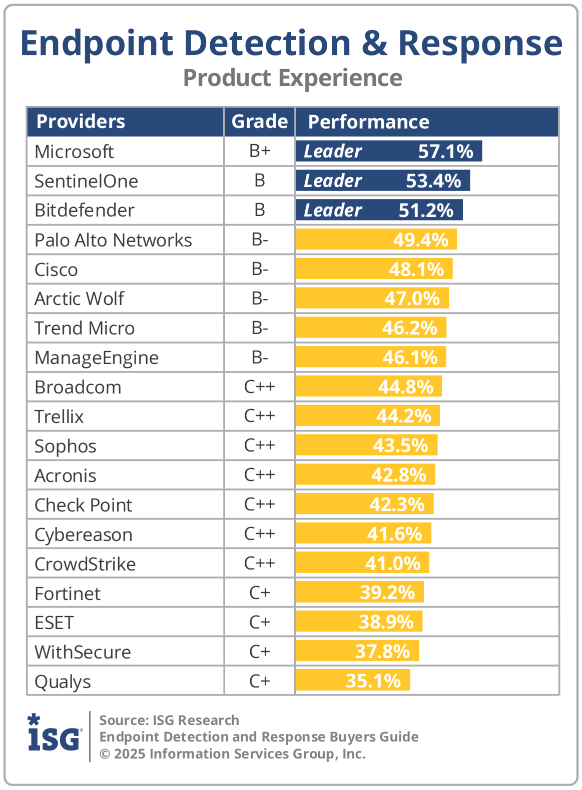
We warn that close provider placement proximity should not be taken to imply that the packages evaluated are functionally identical or equally well suited for use by every enterprise or for a specific process. Although there is a high degree of commonality in how enterprises handle EDR, there are many idiosyncrasies and differences in how they do these functions that can make one software provider's offering a better fit than another's for a particular enterprise's needs.

We advise enterprises to assess and evaluate software providers based on organizational requirements and use this research as a supplement to internal evaluation of a provider and products.

Product Experience

The process of researching products to address an enterprise's needs should be comprehensive. Our Value Index methodology examines Product Experience and how it aligns with an enterprise's life cycle of onboarding, configuration, operations, usage and maintenance. Too often, software providers are not evaluated for the entirety of the product; instead, they are evaluated on market execution and vision of the future, which are flawed since they do not represent an enterprise's requirements but how the provider operates. As more software providers orient to a complete product experience, evaluations will be more robust.

The research results in Product Experience are ranked at 80%, or four-fifths, of the overall rating using the specific underlying weighted category performance. Importance was placed on the categories as follows: Adaptability (8%), Capability (45%), Manageability (9%), Reliability (9%) and Usability (9%). This weighting impacted the resulting overall ratings in this research. Microsoft, SentinelOne and Bitdefender were designated Product Experience Leaders.



Endpoint Detection & Response

Product Experience

Providers	Grade	Performance
Microsoft	B+	*Leader* 57.1%
SentinelOne	B	*Leader* 53.4%
Bitdefender	B	*Leader* 51.2%
Palo Alto Networks	B-	49.4%
Cisco	B-	48.1%
Arctic Wolf	B-	47.0%
Trend Micro	B-	46.2%
ManageEngine	B-	46.1%
Broadcom	C++	44.8%
Trellix	C++	44.2%
Sophos	C++	43.5%
Acronis	C++	42.8%
Check Point	C++	42.3%
Cybereason	C++	41.6%
CrowdStrike	C++	41.0%
Fortinet	C+	39.2%
ESET	C+	38.9%
WithSecure	C+	37.8%
Qualys	C+	35.1%

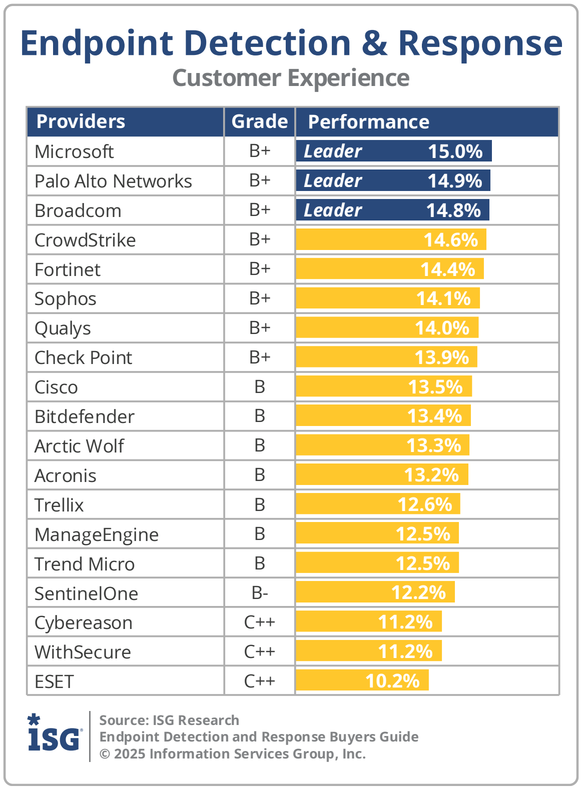
Source: ISG Research
Endpoint Detection and Response Buyers Guide
© 2025 Information Services Group, Inc.

Customer Experience

The importance of a customer relationship with a software provider is essential to the actual success of the products and technology. The advancement of the Customer Experience and the entire life cycle an enterprise has with its software provider is critical for ensuring satisfaction in working with that provider. Technology providers that have chief customer officers are more likely to have greater investments in the customer relationship and focus more on their success. These leaders also need to take responsibility for ensuring this commitment is made abundantly clear on the website and in the buying process and customer journey.

The research results in Customer Experience are ranked at 20%, or one-fifth, using the specific underlying weighted category performance as it relates to the framework of commitment and value to the software provider-customer relationship. The two evaluation categories are Validation (10%) and TCO/ROI (10%), which are weighted to represent their importance to the overall research.

The software providers that evaluated the highest overall in the aggregated and weighted Customer Experience categories are Microsoft, Palo Alto Networks and Broadcom. These category leaders best communicate commitment and dedication to customer needs.



Endpoint Detection & Response
Customer Experience

Providers	Grade	Performance
Microsoft	B+	Leader 15.0%
Palo Alto Networks	B+	Leader 14.9%
Broadcom	B+	Leader 14.8%
CrowdStrike	B+	14.6%
Fortinet	B+	14.4%
Sophos	B+	14.1%
Qualys	B+	14.0%
Check Point	B+	13.9%
Cisco	B	13.5%
Bitdefender	B	13.4%
Arctic Wolf	B	13.3%
Acronis	B	13.2%
Trellix	B	12.6%
ManageEngine	B	12.5%
Trend Micro	B	12.5%
SentinelOne	B-	12.2%
Cybereason	C++	11.2%
WithSecure	C++	11.2%
ESET	C++	10.2%

ISG
Source: ISG Research
Endpoint Detection and Response Buyers Guide
© 2025 Information Services Group, Inc.

Software providers that did not perform well in this category were unable to provide sufficient customer case studies to demonstrate success or articulate their commitment to customer experience and an enterprise's journey. The selection of a software provider means a continuous investment by the enterprise, so a holistic evaluation must include examination of how they support their customer experience.

Appendix: Software Provider Inclusion

For inclusion in the ISG Buyers Guide™ for Endpoint Detection and Response in 2025, a software provider must be in good standing financially and ethically, have at least $100 million in annual or projected revenue verified using independent sources, sell products and provide support on at least two continents and have at least 100 employees. The principal source of the relevant business unit's revenue must be software-related, and there must have been at least one major software release in the past 18 months.

The research is designed to be independent of the specifics of software provider packaging and pricing. To represent the real-world environment in which businesses operate, we include providers that offer suites or packages of products that may include relevant individual modules or applications. If a software provider is actively marketing, selling and developing a product for the general market and it is reflected on the provider's website that the product is within the scope of the research, that provider is automatically evaluated for inclusion.

All software providers that offer relevant EDR products and meet the inclusion requirements were invited to participate in the evaluation process at no cost to them.

Software providers that meet our inclusion criteria but did not completely participate in our Buyers Guide were assessed solely on publicly available information. As this could have a significant impact on classification and ratings, we recommend additional scrutiny when evaluating those providers.

Products Evaluated

Provider	Product Names	Version	Release Month/Year
Acronis	Cyber Protect Cloud	25.05	May 2025
Arctic Wolf	Aurora Endpoint Defense	3.4.1555	June 2025
Bitdefender	GravityZone Endpoint Detection and Response	6.60.1-1	March 2025
Broadcom	Carbon Black EDR Symantec Endpoint Security	7.8.1 N/A	January 2025 February 2025
Check Point	Harmony Endpoint	E88.70 (Windows OS) E89.01 (Mac OS)	March 2025
Cisco	Cisco Secure Endpoint	Secure Endpoint Console 5.4.20241024	October 2024
CrowdStrike	Falcon Insight XDR	7.11	July 2024
Cybereason	Cybereason EDR	Defense Platform 0.1.2000	May 2025
ESET	ESET PROTECT	6.3	May 2025
Fortinet	FortiEDR	7.0	May 2025
ManageEngine	Endpoint Central	11.4.2500	March 2025
Microsoft	Microsoft Defender for Endpoint	platform 4.18.25050.5	June 2025
Palo Alto Networks	Cortex XDR Pro	4.1	April 2025
Qualys	Qualys Endpoint Detection and Response	3.7	April 2025
SentinelOne	Singularity Endpoint	24.2.3.471	April 2025
Sophos	Sophos Endpoint	2025.1.2.12	May 2025
Trellix	Trellix EDR	4.2.2	March 2025
Trend Micro	Trend XDR for Endpoint	14.0.14260	March 2025
WithSecure	WithSecure Elements EDR	25.2.408	April 2025

Providers of Promise

We did not include software providers that, as a result of our research and analysis, did not satisfy the criteria for inclusion in this Buyers Guide. These are listed below as "Providers of Promise."

Provider	Product	Revenue > $100 Million	100+ Employees	Marketed for Large Enterprises
Kaspersky	Kaspersky	Yes	Yes	No
QAX	QAX EDR	No	No	Yes

About ISG Software Research and Advisory

ISG Software Research and Advisory provides market research and coverage of the technology industry, informing enterprises, software and service providers, and investment firms. The ISG Buyers Guides provide insight on software categories and providers that can be used in the RFI/RFP process to assess, evaluate and select software providers.

About ISG Research

ISG Research provides subscription research, advisory, consulting and executive event services focused on market trends and disruptive technologies. ISG Research delivers guidance that helps businesses accelerate growth and create more value. For further information about ISG Research subscriptions, please visit research.isg-one.com.

About ISG

ISG (Nasdaq: III) is a global AI-centered technology research and advisory firm. A trusted partner to more than 900 clients, including 75 of the world's top 100 enterprises, ISG is a long-time leader in technology and business services sourcing that is now at the forefront of leveraging AI to help organizations achieve operational excellence and faster growth. The firm, founded in 2006, is known for its proprietary market data, in-depth knowledge of provider ecosystems, and the expertise of its 1,600 professionals worldwide working together to help clients maximize the value of their technology investments.