IDC MarketScape

# IDC MarketScape: European Managed Detection and Response Services 2024 Vendor Assessment

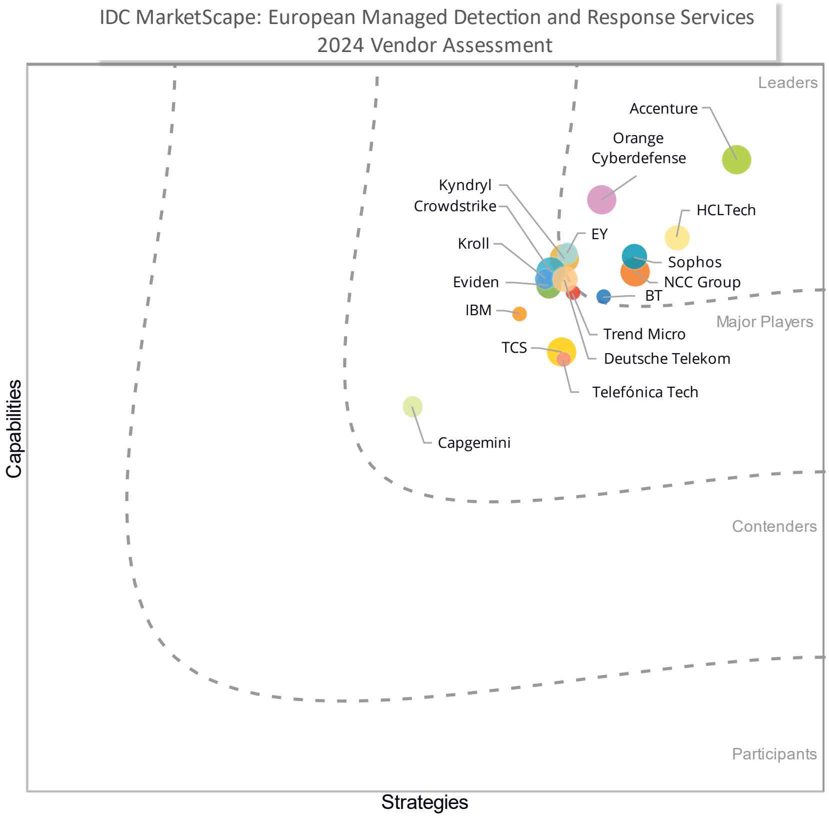
Richard Thurston Joel Stradling Mark Child Romain Fouchereau

## THIS IDC MARKETSCAPE FEATURES SOPHOS

## IDC MARKETSCAPE FIGURE

### FIGURE 1

**IDC MarketScape: European Managed Detection and Response Services 2024 Vendor Assessment**



Source: IDC, 2024

Please see the Appendix for detailed methodology, market definition and scoring criteria.

September 2024, IDC #EUR151172124e

## IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: European Managed Detection and Response Services 2024 Vendor Assessment (Doc #EUR151172124). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

## IDC OPINION

The European managed detection and response (MDR) services market is characterized by a very high level of competition. Barriers to entry for successful service providers are high, but the growth of this market (at a compound annual growth rate of 29.2% from 2022-2027, according to IDC forecasts) has attracted significant numbers of new market entrants alongside more mature players.

The types of players in this market include:

- Dedicated cybersecurity service providers
- Platform vendors
- Professional services companies
- IT services companies or systems integrators
- Network-owning service providers

Each type has something to offer customers in MDR services, though often with different approaches.

This IDC MarketScape focuses on MDR services. Platforms are a part of the evaluation but not the primary focus. There has been some convergence where technology vendors have successfully launched services (often primarily through a channel) and their offer is often substantially different to those of a dedicated service provider. A strong vendor channel strategy will delineate clearly between the service provided by the vendor and the service provided by the service provider. There has, however, been some muddying of the water, and enterprises should clarify roles and responsibilities between the vendor, service provider, and in-house teams as soon as possible.

All of these players have a valid place in the market and are considered in this IDC MarketScape.

In terms of routes to market, it is worth noting that network-owning service providers have, in effect, an internal sales channel for cybersecurity through their telco businesses, and use this successfully to drive the acquisition of MDR customers. This can expand reach across multiple European markets, but all of these players win a large percentage of their revenue from one or two countries.

The IDC MarketScape focuses on comparing service providers from the point of view of a buyer based in Europe. European buyers have unique requirements compared with other regions; a significant proportion of the weighting relates to buyers' specific needs in Europe. While we favorably assess local feet on the ground in European countries, we recognize that it can make sense for providers to deliver some services from outside Europe, for reasons such as the creation of a competency hub or labor arbitrage. Therefore, we keep an open mind about the value of services wherever they are delivered from. We recognize the value, however, of local market understanding, local language support, and knowledge of local regulations.

There is a broad spectrum of approaches for organizations with regards to detection and response, from completely insourced to completely outsourced. Technology vendors can be stronger in deals toward the former end of the spectrum, with service providers seeing their greater success in organizations where external value-add is sought. In practice, nearly all organizations will benefit from at least some element of outsourcing. Whether to do so depends on budget, in-house resources, and the choice of service provider. Outsourcing is not necessarily more expensive and can deliver considerable additional value for an organization compared with an in-house approach, even before the cost of security incidents is considered.

It is common — and advised — for service providers to partner with other technology or service organizations to enhance their MDR services offers. This causes some muddying of the waters as some service providers in this IDC MarketScape collaborate with each other. An organization might contract with a service provider that partners with the platform vendor, or with the platform vendor directly.

In evaluating each provider, we are primarily interested in the services that they bring. Their choice of partner is recognized within the scoring mechanism.

As a services-focused IDC MarketScape, this document does not exhaustively cover MDR platforms, of which there are many in the market. We include three technology vendors in this report because of the services they offer; each company's platform is strong. Readers should not interpret the overall rating as a reflection purely of the platform.

This IDC MarketScape is not an exercise in price benchmarking. Complex corporate services can deliver a great deal of organizational value and are priced much higher than simpler services aimed at SMEs. However, due to the variables involved, price benchmarking should be undertaken as a custom exercise, and we do not include price as a criteria in this IDC MarketScape. Organizations should recognize that a complex managed service for a large enterprise will be very different to a more commoditized SME offer, for example. Both have merits for the right buyer and organizations should identify their specific needs and conduct their own due diligence. IDC can provide price benchmarking as a separate activity.

Finally, it is worth noting that there are many acronyms in the detection and response market. We refer to MDR services, but we also see:

- Extended detection and response (XDR) or managed extended detection and response (MXDR), which tend to refer to capabilities based around a platform
- Threat detection and response (TDR), which is assessed where it is provided as a service

IDC published a related IDC MarketScape in 2022 covering European managed security services, which from a taxonomy point of view is a superset of this IDC MarketScape. Due to changing market circumstances, including different players and different criteria weightings, it would not be helpful to directly compare the positions of providers as a time series with this IDC MarketScape.

## IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Due to high levels of competition in the European MDR Services market, barriers to entry for this IDC MarketScape are high, so the 17 qualifying service providers are under the Leaders and Major Players category.

IDC had produced a list of significant service providers in the European MDR services market based on their capabilities and success in supporting European organizations. All these service providers were invited to answer a qualification questionnaire from which successful service providers were included in this IDC MarketScape. To qualify for the IDC MarketScape, service providers had to meet all of the following inclusion criteria:

- Must sell MDR services to end-user businesses or public sector organizations in Europe
- Must offer support in Europe when a customer requests it or offer support for its MDR services during European working hours
- Must have MDR services customers in at least three of the largest five European economies (France, Germany, Italy, Spain, and the U.K.)
- Must meet at least one of the two following conditions:
  - Must have annual revenue from MDR services sold to end-user businesses and public sector organizations in Europe of over $20 million and at least 50 employees based in Europe and dedicated to the sales, presales, engineering, design, provision, or ongoing management of MDR services to end-user businesses and public sector organizations in Europe
  - Must have annual revenue from MDR services sold to end-user businesses and public sector organizations in Europe of over $10 million and at least

200 employees based in Europe and dedicated to the sales, presales, engineering, design, provision, or ongoing management of MDR services to end-user businesses and public sector organizations in Europe

Organizations with specific needs, operating in specific geographic areas, or whose base is primarily outside of Europe may find value in the offerings of other service providers.

## ADVICE FOR TECHNOLOGY BUYERS

We recommend that buyers read thoroughly the vendor summary profiles and review the IDC MarketScape chart. There is a large amount of qualitative and quantitative detail behind this assessment. There are many nuances in the provision of MDR services and buyers should map on their own objectives and risk profile when selecting a service provider.

Considerations may include:

- **The required delivery model.** How hands-off do you want to be? Are you looking for a fully outsourced service, or an extension to your security operations center (SOC) team?
- **Wider services required.** These vary hugely, which forms a basis for our analysis. Global IT services companies will offer a broad suite of complementary services, while MDR services specialists will be much more focused. Professional security services such as preparedness and incident response (IR) are highly relevant here.
- **Data sovereignty requirements.** How can the service provider guarantee to meet your needs? This may refer to EU or single-country regulations.
- **AI/ML road map.** These technologies are not new, but capabilities in generative AI (GenAI) and automation are evolving rapidly. Ask your service provider for their road map.
- **Language support.** Security incidents and crises are stressful and certainly not a time for miscommunication. Ensure your service provider can support your people in their chosen language through the full life cycle of the services you procure.
- **Trust.** This is a very personal consideration around what type of provider you want to work with in pressure situations and it tends to drive different purchasing behaviors. Establish playbooks and processes in advance. When will the provider call your organization? What actions will they take automatically?

## VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each criterion outlined in the Appendix, the description here provides a summary of each vendor's strengths and opportunities.

### Sophos

Sophos is positioned in the Leaders category in the 2024 IDC MarketScape for European MDR services.

Sophos launched the first version of its MDR offering, branded Sophos Managed Threat Response, in October 2019. This was later rebranded to Sophos MDR in November 2022 with an expanded offering and the ability to work with third-party event sources and components. Sophos has built out its MDR capabilities and offerings both organically and with a series of acquisitions, including Capsule8 for Linux Detection and Response, Braintrace for network detection and response, and Refactr for SOAR and process automation (all in 2H21). The vendor also acquired SOC.OS for security alert correlation and triage automation in 2022. The company has more than 23,000 MDR customers worldwide, making it one of the biggest players on the market in terms of customer base. In Europe, it counted more than 5,000 unique MDR customers at the end of 2023, with the majority being under-250-employee organizations. Most of these are contracted through its channel, but the service is delivered by Sophos itself.

Sophos provides human-led threat response as part of the core of its MDR service offering. This includes a broad range of response actions from isolating hosts and terminating processes to root cause analysis, malware analysis, and the provision of a dedicated IR team. The vendor has SOCs in UK&I and Germany certified for SOC2 Type II and PCI DSS. The Sophos IR service is accredited with the UK National Cyber Security Centre (NCSC) Cyber Incident Response (CIR) Level 2 for U.K. public and private sector organizations and is a qualified APT response service provider for critical infrastructure operators in Germany.

Where the customer has a Sophos agent deployed or Sophos proprietary tools, the Sophos MDR service draws data directly from endpoints, network, cloud, email, some IoT and OT environments, and third-party data collected through APIs or a third-party log collector. This includes, for example, firewall data or SIEM data from Microsoft Sentinel. Where there is no agent or Sophos tool, the service can still collect third-party data. Data is correlated, passed through Sophos' rule engine, and stored in its data lake. Regarding storage, 90 days is the default, with an optional one-year extension available at a premium.

A key differentiator for any MDR service is its incident response component. Sophos emphasizes that unlimited IR is a core service, although the extent of this depends upon the service tier. For MDR Complete customers, this means full-scale incident response with all threats fully eliminated. MDR Essentials customers get a threat response service, which commits to stopping and containing all active attacks. MDR Essentials customers may also choose to purchase an IR retainer for the extra coverage on top of the core service components they receive. This means that customers that start out with MDR Essentials but decide they want or need more have two options: add the IR retainer or upgrade to the full MDR Complete service (with all the additional components that brings).

Regarding data residency, Sophos processes telemetry in the region in which the customer account is provisioned. For Europe, Sophos is hosted in the UKI and Germany AWS regions.

Finally, it is worth noting the work that Sophos has done in the partnerships and alliances area:

- Like many vendors, Sophos has looked for ways to complement or extend capabilities around Microsoft. It offers an MDR for Microsoft Defender service, with a team monitoring, investigating, and responding to Microsoft Defender alerts and integrating multiple Microsoft Security event sources. The vendor has also worked on numerous use cases around Microsoft telemetry, such as email compromise, as it aims to deliver concrete security benefits to its clients. Sophos MDR also includes an integration with Microsoft Graph Security API (for customers that have an E5 license); this integration is included in the standard price of all MDR subscriptions.
- Sophos similarly has integrations with Google Workspace, with analysts conducting investigation and response for security events sourced from Workspace. This reinforces Sophos' credentials in the small business segment, where many organizations use Google Workspace rather than Microsoft. As with the Microsoft integrations, the Google Workspace integration is provided at no additional cost.
- A new development is an alliance with backup player Veeam. Sophos believes it is the first MDR player to partner with Veeam or any other backup player for MDR (and has deals with more backup providers in the pipeline). According to research conducted by Veeam, 75% of ransomware attacks impact backups, which indicates that Sophos could be addressing a very underserved part of the technology stack. The two vendors reportedly have substantial partner and customer overlap and have therefore been able to work rapidly together to develop use cases.
- In April 2024, Sophos announced a strategic partnership with Tenable to launch Sophos Managed Risk, a vulnerability and attack surface management service. With a dedicated Sophos team leveraging Tenable's exposure management technology the companies aim to drive collaborative operation between MDR and vulnerability management. With extensive reporting and prioritization around vulnerabilities, this should help sort signal from noise

and address use cases such as risk mitigation through attack surface visibility, patch prioritization, and rapid identification of new risks through alerts around new critical vulnerabilities.

## Strengths

Sophos has built its MDR business on the back of a strong technology platform, as a long-established player in the endpoint and network security segments, subsequently expanding into XDR. Nevertheless, Sophos' MDR approach is not limited to customers using its proprietary security technologies: it can also go to market as a technology-agnostic service provider, at least for customers adopting its entry-level MDR Essentials service offering. Customers that adopt the premium MDR Complete service need to be running the full Sophos XDR agent, to get all the additional benefits and capabilities that Complete provides. These include root cause analysis, full-scale incident response, a dedicated incident response lead, and a Sophos breach protection warranty.

Sophos has built a very strong position in the midmarket, with more than two-thirds of its MDR customer base among organizations with up to 250 employees, and almost a fifth in the 250–999 employee segment. With more than a thousand partners reselling Sophos MDR in Europe, the vendor is well positioned to continue targeting an extensive segment of the market that its enterprise competitors may not have the reach to address.

## Challenges

Sophos has built one of the biggest global MDR businesses on the market by the number of customers. Nevertheless, when comparing the European service coverage with that of North America, the levels of operation are markedly different. Sophos' SOC representation in North America comprises more than 150 FTEs, operating 24 x 7 x 365. In comparison, SOC representation in Europe, with analysts based in the U.K., Ireland, and Germany, stands at around 34 FTEs, with 8 x 5 availability. Sophos also has solid headcount in India (more than 70 FTEs operating 24 x 7 x 365) and further presence in Australia, so the vendor can offer round-the-clock support. Nevertheless, European prospects demanding more extensive in-region support may raise concerns about this aspect of the service. Sophos emphasizes that it is aiming to build more capability through partners, but concrete details of this have not yet been announced.

## Consider Sophos When

With decades of experience and knowledge as a security technology vendor, Sophos has considerable expertise when it comes to how cyberattacks impact and unfold across enterprise infrastructure. Since the launch of its MDR ambitions with a series of acquisitions in 2019, the vendor has also put considerable emphasis on building teams of highly experienced and skilled security analysts to deliver its human-led service. The company's unmetered and unlimited incident response offering is a compelling component of this. Where organizations are seeking an MDR provider with deep security expertise and a human-led service that engages with them from the outset until an incident has been resolved, Sophos represents a compelling option.

## APPENDIX

### Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the Y-axis reflects the service provider's current capabilities and menu of services and how well aligned the service provider is to customer needs. The capabilities category focuses on the capabilities of the company and service here and now. Under this category, IDC analysts will look at how well a service provider is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the X-axis (strategies axis) indicates how well the service provider's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual service provider markers in the IDC MarketScape represent the MDR Services market share of each individual provider. There are five gradations.

### IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and service provider scores represent well-researched IDC judgment about the market and specific service providers. IDC analysts tailor the range of standard characteristics by which service providers are measured through structured discussions, surveys, and interviews with market leaders, participants and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual service provider scores — and ultimately service provider positions on the IDC MarketScape — on detailed surveys and interviews with service providers, publicly available information, and end-user experiences to provide an accurate and consistent assessment of each service provider's characteristics, behavior, and capability.

### Market Definition

Managed detection and response (MDR) services — a subset of managed security services (MSS) as per IDC's Security Services taxonomy — combines the tools, technologies, procedures, and methodologies used to provide full cybersecurity detection and response capabilities for an organization. There must be a set of services provided to the client on top of the product or platform for it to be considered in this IDC MarketScape, and, while the platform is an integral part of the offer to the client, it is primarily the set of services that is evaluated in this report.

While service providers' global capabilities are assessed, the focus of this IDC MarketScape is MDR services that can be delivered for businesses and public sector organizations with locations in Europe.

## LEARN MORE

### Related Research

- *European Security Services Forecast 2024-2028* (IDC #EUR150685524, June 2024)
- *Managed Detection and Response Services in Europe: Standing Out in a Growing but Congested Market* (IDC #EUR151225123, September 2023)
- *Incident Response: A Key Growth Driver for European Professional Security Services — How IR Plays a Critical Role in Organizational Resilience* (IDC #EUR150794623, June 2023)
- *EMEA Security Services Survey, 2024: Selected Results* (IDC #EUR151778023, February 2024)
- *IDC's Worldwide Security Services Taxonomy, 2024* (IDC #US50636024, June 2024)

### Synopsis

This IDC MarketScape assesses the major providers of managed detection and response (MDR) services for organizations operating in Europe. Detecting and responding to cybersecurity threats promptly and effectively is essential for organizations. Many do not have the knowledge or resources in house to do this successfully, so are working with one of many service providers. These service providers bring substantial expertise and are helping organizations mitigate cyber-risk.

"The MDR market is complex and competitive, with a huge array of impressive services on offer," said Richard Thurston, research manager, European Security Services, IDC. "However, organizations must choose carefully to ensure they work with a service provider that delivers on their business and technology objectives. This will include decisions around technical capabilities, services, and skill sets; target market; and their strategic road map."

## ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

## IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
blogs.idc.com
www.idc.com

### Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/about/worldwideoffices. Please contact IDC report sales at +1.508.988.7988 or www.idc.com/?modal=contact_repsales for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.