

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

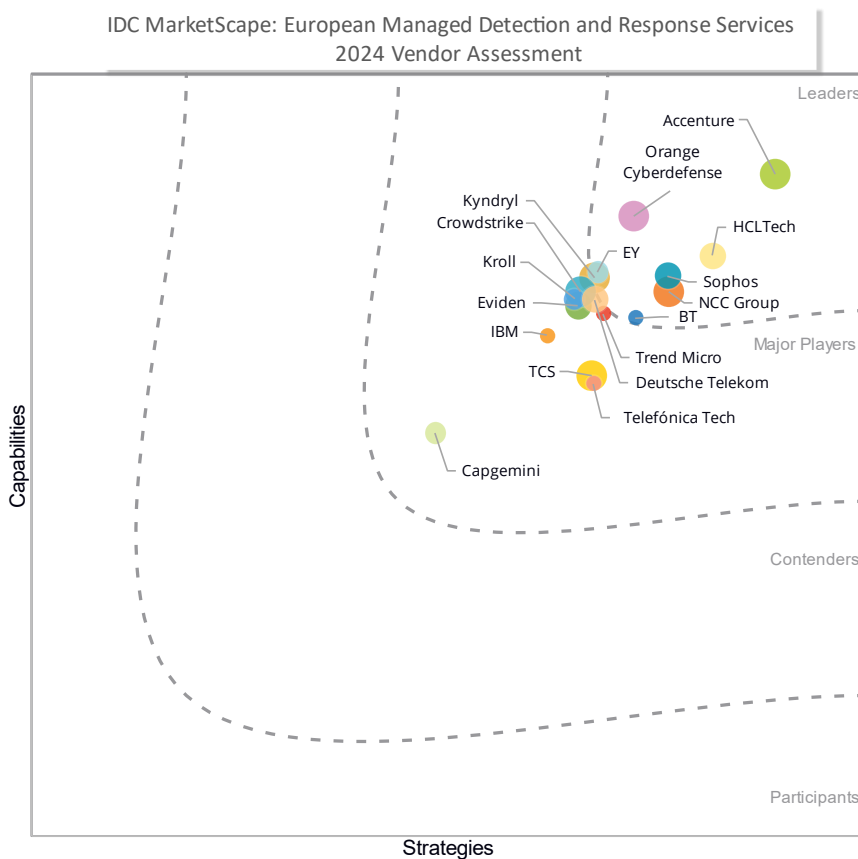
Richard Thurston Joel Stradling Mark Child Romain Fouchereau

THIS IDC MARKETSCAPE EXCERPT FEATURES ACCENTURE

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.

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 PROFILE

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.

Accenture

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

The multibillion-dollar Accenture business offers a far wider set of services than cybersecurity, but cybersecurity is a fast-growing line of business; it has been providing some form of detection and response services for more than 20 years and has 1,300 employees in Europe involved in detection and response roles. Accenture provides cybersecurity services globally, with an in-depth presence in Europe, working across eight languages.

Its security offer is grouped broadly under strategy, protection (including zero-trust principles to support digital transformation), vertical sector offerings, industrial security (operational technology or OT), resilience (which includes MDR), and the emerging area of quantum security.

Resilience (and more generally, the alignment of cybersecurity and business risk) remains the objective for that pillar, and MDR (which it calls Threat Detection and Response) is deployed to facilitate that. Threat exposure management, transformation, response readiness, incident and forensic response, crisis management, and threat intelligence complete the set of Accenture's resilience services.

It provides MDR through 21 centers for detection and response sites that operate as either security operation centers or Cyber Fusion Centers (CFCs).

The MDR offering comes with two primary design principles:

- The first is its Extended concept (i.e., it extends clients' capabilities beyond what they previously had). Extended telemetry intakes and protections are provided to the client's environment beyond the traditional network or endpoint devices. IT, OT, and IoT environments are monitored and protected.
- The second is its Adaptive model. The service is designed to ensure that the client has access to the right technologies without getting into a vendor lock-in situation. It can integrate into a client's existing tools while leveraging its industry-specific capabilities.
- Accenture offers a SOC content co-creation workshop to help clients design the right operating model and shape their capability development road map.

The company also offers multiple licensing options for service and platform elements depending on full-stack or hybrid service options, with the former including a full technology-as-a-service stack and the latter integrating with client-owned tools. These include ingestion-based licensing (e.g., clients on Splunk and Google), consumption-based licensing (e.g., clients on Microsoft Sentinel), and based on company size (all-you-can-eat for their full-stack clients, number of employees for clients on Google SIEM).

Accenture's offering is a modular, cloud-native, and outcome-based MDR service. It also features pricing flexibility to customize to clients' budgets while leveraging existing client technology investments.

The incident response team is preconfigured with break-glass access to tools and systems to enable the rapid collection and analysis of forensic images, artifacts, logs, and other data to support the investigation. There is a regular cadence for update calls between the client and the IR team, and the IR team is in constant communication with the SOC to carry out actions to contain, eradicate, and remediate the potential threat.

Accenture is embedding generative AI across its life cycle via targeted use cases around guided collection and analysis. These use cases are designed to increase throughput of threat hunting missions, reduce manual steps across the hunter life cycle, and increase threat hunter efficiency. It has developed threat hunting use cases with GenAI and it is anticipated that these will continue to be leveraged in production in the next 18 to 24 months.

It is investing heavily in AI as an organization, which, along with its partners' AI innovations, can be expected to filter through into benefits for MDR clients. Accenture plans to double the number of AI professionals to 80,000 as part of a \$3 billion program.

Accenture has made a significant investment in its Content Factory team within its Detection and Response organization. This team leverages agile and detection-as-code methodologies to deliver new content rapidly, customizing it to meet clients' specific needs.

Over time, Accenture has built its own cybersecurity intellectual property and acquired organizations that can add breadth or depth to its capabilities. Recent examples include the acquisition of Symantec Global Managed Security Services, Context Information Security in the U.K., and Revolutionary Security (with a focus on OT/IoT security) in 2020; Openminded and Linkbynet in France in 2021; Sentor in Sweden in 2021; and Innotec in Spain in 2023 (threat simulation, detection, response and incident management, cyber-intelligence, infrastructure and application security, cyber-risk assessment, and security consulting).

Strengths

Accenture brings significant industry and historical experience to tailor its offering and offers prescriptive guidance to tailor its services to clients' needs. Its scale means it can adapt where the service is delivered from, for example, because of data sovereignty, geopolitical, or support requirements, which helps it align with a greater number of client objectives.

It can replicate best practices globally but has the feet and knowledge on the ground in-region to support European businesses. Within Europe, it has Cyber Fusion

Centers and SOCs in Spain, Italy, France, the U.K., Sweden, Finland, and Czech Republic and its cybersecurity customer list is extensive across major European markets.

The lines are blurring between traditional consulting and managed services such as MDR. Given its strong set of professional and managed services, this may play in Accenture's favor.

Accenture possesses a high number of strong vendor partnerships, from cloud hyperscalers to security vendors, as well as a portfolio from which it can pull to support different client needs. This approach can reduce the risk of vendor lock-in to organizations.

It has a large content library, consisting of detection use cases, playbooks, threat hunting models, reports, and dashboards, which can be used from the start of service. All content can then be customized based on clients' needs, applications, and processes.

Accenture produces considerable volumes of informed and relevant thought leadership, which is likely to increase consideration of its services.

Accenture was one of the few service providers to include an HR leader in its briefing for this IDC MarketScape, which underlines the importance of its people-led approach and its focus on diverse talent retention. It was also one of the most expansive regarding strategy, and provided considerable detail on offerings, progress, and best practices.

Challenges

Due to the scale of the organization, we would envisage that smaller players would usually have greater success in the SME market.

Consider Accenture When

Due to the breadth of its portfolio, Accenture is well placed to support clients with needs covering adjacent business issues such as crisis management, cloud, AI, technology strategy, supply chain considerations, talent, and broader technology transformation alongside cybersecurity. It often provides its security people for projects that have a wider business purpose and mandates the inclusion of security teams on those projects in some circumstances.

It has considerable expertise across all key vertical markets, so should be considered by organizations with sector-specific requirements. The financial services vertical provides the largest amount of revenue by sector.

Global organizations with a strong European presence should also consider Accenture due to its scale, best practices, and experience in delivering outcomes for large enterprises.

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.

Copyright 2024 IDC. Reproduction is forbidden unless authorized. All rights reserved.