IDC MarketScape

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

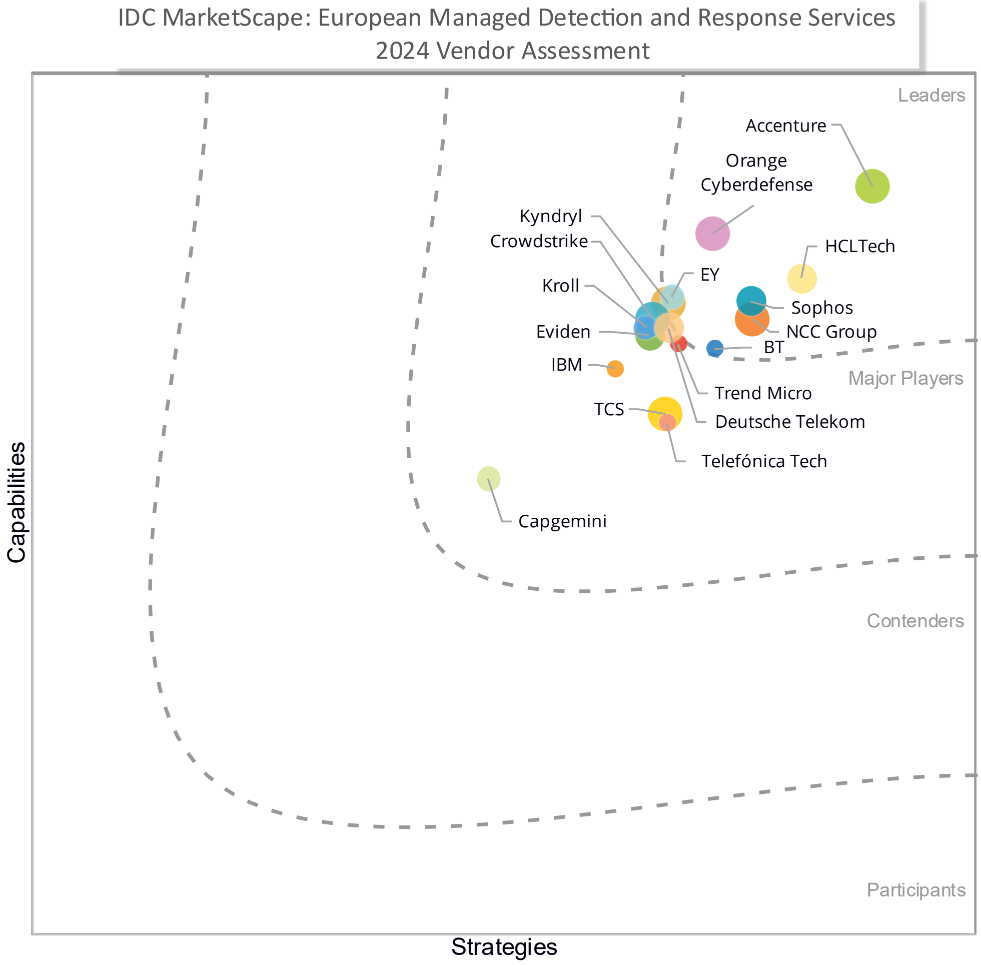
Richard Thurston Joel Stradling Mark Child Romain Fouchereau

THIS EXCERPT FEATURES EY AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

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



Source: IDC, 2024

September 2024, IDC #EUR151172124e

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

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: European Managed Detection and Response Services 2024 Vendor Assessment (Doc # EUR151172124).

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.

EY

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

EY receives many requests from organizations looking for independent assurance of their cybersecurity posture. It performs security assessments as part of all its managed services offerings, which helps it to provide ongoing cybersecurity posture improvements and risk mitigation.

Its cybersecurity offerings can be enhanced with proactive services aligned to industry sectors. Cybersecurity managed services sit within EY's technology consulting offering and are aimed at helping businesses transform their cybersecurity programs to meet business objectives, such as to build greater resilience, digital trust and long-term value (through better insights into cyber-risk). It does this through people, processes, technology, and alliances. EY's focus is to transform the security function from a cost center to a business enabler, leveraging its "transform through operate" approach.

Its cybersecurity managed services are focused on four areas:

- Supply chain risk
- MDR (which it calls threat detection and response or TDR)
- Threat exposure management
- Digital identity

In line with most other market offers, EY's TDR service aims to:

- Detect advanced cyberthreats
- Undertake automation and orchestration that enhances the ability to find, hunt and respond to indicators of attack and compromise
- Optimized logging of incidents, creation of watchlists, and curation of threat-centric use cases
- Reporting and intelligence-based recommendations to better prevent or mitigate cyberattacks.

For most clients, TDR will form part of a set of services procured from EY. EY primarily focuses on cross-selling to its existing consulting and professional services clients across assurance, tax, and strategy and transactions service lines, rather than net-new customers.

Beyond cybersecurity managed services, EY can (if needed) offer services from its Law & Legal Managed Services team, or Forensics and Cyber Assurance. There is already considerable work undertaken within EY's Cyber Assurance and Forensics and Integrity service teams as well as its enterprise risk management, internal audit, and risk control teams. EY intends to further consolidate and operationalize these efforts in 2024.

From a people perspective, EY has over 13,700 cybersecurity practitioners; in terms of local client support, it deploys consultants in the country of the client's leadership team where possible (though core competencies may be centralized for effectiveness). Its European security diversity, equity, and inclusion initiatives include the Cyb-her initiative, with a dedicated number of female head count.

Services can be co-sourced with EY people working alongside internal teams, which can be for out-of-hours only, or outsourced 24 x 7 x 365.

Since 2020, EY has opened Nearshore Delivery Centers in Newcastle (U.K.), Malaga (Spain), Dublin (Republic of Ireland), and Warsaw (Poland) that service MDR clients. It also provides niche or specialist support, including OT MDR services, enabling it to meet regulatory compliance needs around NIS 2.0, the EU AI Act, and the EU Data Act, for example. It operates five European SOCs and has 37 cyber delivery centers across the EMEIA region (Europe, the Middle East, India, and Africa). It has labs dedicated to threat intelligence, incident response, and forensics. Its flagship SOC is in Malaga, with this center acting as a central hub across EU-country specific SOCs; this SOC integrates with EY's global network of SOCs.

EY has incorporated multiple practices and technologies into its MDR service. For example, the company can also offer threat and vulnerability identification in parallel with MDR. EY offers clients more than 1,300 cases of detection logic aligned to the MITRE ATT&CK framework. EY can also extend regular evaluation of vendor-native and EY-developed detection logic, unified kill chain, threat modeling, client-specific intelligence profiles, and continuous threat hunting with orchestration and automation leveraging SOAR, advanced analytics, AI, ML, and user (and entity) behavior analytics (UBA/UEBA). These practices and technologies enable EY's risk-based triage, analysis, remediation and threat disruption capabilities.

OT is a growing focus for many organizations. In response to this, EY supports clients seeking coverage for standalone IT, standalone OT, and hybrid IT-OT environments.

EY has an extensive SOAR use case library that includes more than 400 playbooks originating from its SOAR Center of Excellence. It also has over 100 out-of-the-box integrations with threat intelligence, EDR, SIEM, and cloud posture management tooling. EY will likely add several threat intelligence sources to its TDR value proposition over the next 18 months.

EY optimizes commercial off-the-shelf SIEM, EDR, XDR, and NSM/NDR technologies to deliver its MDR services. It does not deploy proprietary EY-owned platforms, but does deploy EY workflows, dashboards/workbooks, detection logic, and correlation logic/use cases to further vendors' capabilities.

Major partners include CrowdStrike, Tanium, Microsoft, ServiceNow, Splunk, and Saviynt.

In terms of AI investments, the EY organization announced in 2023 a $1.4 billion firmwide investment in its EY.ai ecosystem.

From an MDR perspective, EY has invested in accelerators that include a predictive AI decision engine for threat response, an SOC-as-code orchestrator, more than 50 custom ML-based threat hunting notebooks, and an attack disruption toolkit.

In the future, IDC expects EY to focus more on a sector-specific go-to-market approach, instead of the previous solution-based approach, which should help address industry-specific challenges around regulation and use cases.

Strengths

EY has strong business relationships at senior levels and is well-placed to support multinational organizations in transforming their cybersecurity operations and driving value from the security function. It can provide services that support many adjacent business objectives. Its investment in AI and ML is large, and progress in AI is driving forward its cybersecurity services. The more expected cyber-risk quantification capabilities, and perhaps less-expected OT security capabilities, are further strengths for EY.

Challenges

Smaller businesses or those with more niche or very cybersecurity-specific requirements may not have the scale to align with the EY MDR service.

Consider EY When

Multinational enterprises with an existing EY engagement seeking assistance with strategic cybersecurity transformation and operations should consider EY.

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