LANDSCAPE REPORT

The Managed Detection And Response Services In Europe Landscape, Q2 2025

Forrester's Overview Of 25 Providers

May 1, 2025

By Tope Olufon with Jinan Budge, Min Say, Angela Lozada, Bill Nagel

FORRESTER®

Summary

You can use managed detection and response (MDR) services in Europe to rapidly detect, investigate, and respond to unauthorized or suspicious activity; assure customers via threat-hunting that adversaries haven't gained access; and recommend actions to improve your overall security posture. But to realize these benefits, you'll first have to select from a diverse set of providers that vary by size, type of offering, geography, and business scenario differentiation. Security and risk (S&R) professionals should use this report to understand the value they can expect from an MDR service provider in Europe, learn how providers differ, and investigate options based on size and market focus.

Market Definition

Managed detection and response service providers help relieve constraints on a client's resources and skills, security team, and security operations center (SOC). S&R professionals seek providers that bring expert security practitioners with visibility into global and European threats and threat actors, detection engineering skills, and strong threat-hunting capabilities and have technologies to manage a fluid, complex threat ecosystem at scale. Forrester defines managed detection and response services as:

Services that augment extended detection and response (XDR) tools with telemetry from network, identity, cloud, APIs, applications, and other log sources to produce high-fidelity detections, conduct investigations, support remote incident response, enable security automation, initiate threat hunts to identify adversaries that circumvent security controls, and help improve their clients' overall security posture.

S&R professionals in Europe use MDR service providers to obtain 24/7 security monitoring, enhance SOC expertise, assist with or lead incident response, provide stability when people leave the organization, achieve threat-hunting objectives, provide assurance that sophisticated adversaries and embedded threats are not in the system, and strategically shape security direction by identifying gaps and prioritizing improvements.

Business Value

Managed detection and response service providers help security teams reduce attackers' inherent advantage in an asymmetric security landscape by enhancing the security team's ability to protect the customers, employees, partners, suppliers, and investors in their business ecosystem. S&R pros in Europe implement MDR services to:

- **Rapidly detect, investigate, and respond to unauthorized or suspicious activity.** MDR service providers bundle network traffic insights, behavioral analytics, threat intelligence, and deep technical expertise into actionable information used to generate alerts, aid forensics, and guide incident response efforts. MDR service providers sometimes also execute incident response for their clients; providers' delivery capacity and specialization eases some of the pressure on customers, as providers operate at larger scale and have broader insights.
- **Assure customers via threat-hunting that adversaries haven't gained access.** Persistence is a key element of threat actors' efforts to compromise security; it saves time and ensures "recurring revenue." To combat this, firms need assurance that not only has the immediate threat been neutralized but that embedded threat

actors have been identified and eliminated. MDR service providers do this with human-led, hypothesis-driven threat-hunting that goes beyond analytics and draws on experience and creative efforts to find indicators of compromise or beacons.

- **Recommend actions to improve overall security posture.** MDR service providers furnish insights to improve organizations' security posture. Data obtained from monitoring, detection, and analysis of the threats handled can yield practical recommendations and help security leaders prioritize their initiatives. Good MDR service providers don't just tell you something's broken; they help you prioritize the fix.

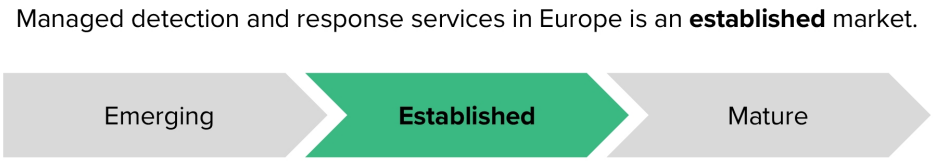
Market Maturity

For European firms, managed detection and response is no longer optional; it's a necessity. To get an edge in an increasingly competitive and crowded ecosystem, MDR service providers in Europe have diversified their portfolios to also offer services like attack surface mapping and breach assessments. MDR services in Europe has evolved into an established market where (see Figure 1):

- **Resilience is emerging as a core differentiator.** European firms increasingly focus on maintaining operational continuity as regulations like the EU's Network and Information Security 2 (NIS 2) directive push for more resilient ecosystems. In response, MDR service providers are adding resilience-focused offerings such as threat simulations and breach assessments to guide tailored recovery planning. Services like attack surface mapping and exposure management have become common add-ons to aid discovery and enable proactive defense.
- **Basic detection and response capabilities are commoditizing.** The market has outgrown traditional endpoint detection and response; security operations now relies on diverse telemetry sources to inform proactive defense strategies with XDR, expanding the technology to ingest diverse data sources and produce data-driven insights to enable proactive threat containment.
- **Identity-driven detection and response is a priority.** Significant numbers of breaches involve credential abuse, making identity an essential element of security architecture and a valuable asset in the hands of threat actors. European MDR service providers now emphasize identity-centric monitoring and response capabilities in addition to traditional endpoint and network-centered activities, creating a foundation for richer analytics and more data-driven playbook creation.

Figure 1

Managed Detection And Response Services In Europe Market Maturity And Key Dynamics



Key market dynamics

MAIN TREND	PRIMARY CHALLENGE	TOP DISRUPTOR
European firms consider extended detection to be an essential capability.	Providers rush to plug the talent gap with AI, aiding detection but not response.	Smaller providers using geography and specialization as selling points.

Market Dynamics

As the highly competitive European MDR market matures, customers expect more services and capabilities from their MDR service providers at a lower cost. This competition drives providers to get creative with solution offerings, bundling, and pricing as they try to stay ahead of each other and retain market share. S&R professionals will face a plethora of provider options and should pay attention to the following market dynamics:

- **Main trend.** European firms consider extended detection to be an essential capability. XDR is a baseline expectation of European organizations prioritizing broad, integrated telemetry across endpoints, cloud, applications, and identity. As regulatory pressures increase and security leaders become accountable for security breaches, European customers expect MDR service providers to back telemetry with threat intelligence, deliver rich insights, provide deep response capabilities, and use these to increase organizational resilience.
- **Primary challenge.** Providers rush to plug the talent gap with AI, aiding detection but not response. Generative AI has failed to solve the problems that arise due to

personnel gaps. Moreover, its effectiveness, especially in response actions, leaves much to be desired; AI is not yet capable of providing the nuance and context required for incident response. This forces customers to sift through hype, marketing, and glib presentations to find a provider that will help them respond to incidents faster and more effectively.

- **Top disruptor.** Smaller providers using geography and specialization as selling points. As the market matures, specialized regional providers have emerged as competitive threats due to concerns around data sovereignty, price, language, and cultural expectations. While dominant players still lead in terms of scale and functionality, niche providers offer much-needed service localization, understanding of the local regulatory and threat landscape, and services at more locally sensitive price points.

Notable Providers

Security and risk professionals can start investigating specific providers based on their geographic focus, industry focus, deployment options, and size. Across all markets, Forrester defines large providers as having $250 million or more in annual category revenue, medium providers as having $100 million to less than $250 million, and small providers as having $10 million to less than $100 million (see Figure 2).

Figure 2

The Managed Detection And Response Services In Europe Landscape, Q2 2025

Provider	Geographic focus	Industry focus	Type of partner	Size
Accenture[1]	EMEA: Northern Europe; EMEA: Western Europe	Financial services Manufacturing/production of high-tech products Retail	On-premises Hosted, private SaaS Multitenant SaaS	■ ■
Bitdefender	EMEA: Northern Europe; EMEA: Western Europe	Education and social services Healthcare Manufacturing/production of industrial products	Multitenant SaaS	■
BlueVoyant	EMEA: Northern Europe; EMEA: Western Europe	Financial services Healthcare Pharmaceuticals and medical equipment	Multitenant SaaS	■
CGI[1]	EMEA: Northern Europe; EMEA: Western Europe	Government Telecommunications Utilities	On-premises Hosted, private SaaS Multitenant SaaS	■
CrowdStrike	EMEA: Northern Europe; EMEA: Western Europe	Financial services Healthcare Manufacturing/production of high-tech products	Multitenant SaaS	■ ■
CyberProof	EMEA: Northern Europe; EMEA: Southern Europe; EMEA: Western Europe	Financial services Healthcare Retail	On-premises Hosted, private SaaS Multitenant SaaS	■
Deutsche Telekom	EMEA: Eastern Europe; EMEA: Western Europe	Healthcare Manufacturing/production of industrial products Retail	On-premises Hosted, private SaaS Multitenant SaaS	■ ■
eSentire	EMEA: Northern Europe; EMEA: Western Europe	Financial services Healthcare Manufacturing/production of industrial products	On-premises Hosted, private SaaS Multitenant SaaS	■
ESET	EMEA: Western Europe	Financial services Healthcare Manufacturing/production of industrial products	On-premises Multitenant SaaS	■

Size ■ ■ ■ Large ≥$250M ■ ■ Medium $100M to <$250M ■ Small $10M to <$100M

Note: Geographic focus indicates regions where the provider's product revenue in this category is greater than or equal to 15% of its total product revenue.

1. The information about this provider includes Forrester's estimates.

Provider	Geographic focus	Industry focus	Type of partner	Size
EY[1]	EMEA: Northern Europe; EMEA: Southern Europe; EMEA: Western Europe	Government Manufacturing/production of industrial products Pharmaceuticals and medical equipment	On-premises Hosted, private SaaS Multitenant SaaS	■
HCLTech[1]	EMEA: Northern Europe; EMEA: Western Europe	Financial services Healthcare Manufacturing/production of high-tech products	Multitenant SaaS	■
I-TRACING[1]	EMEA: Western Europe	Financial services Retail	On-premises Hosted, private SaaS Multitenant SaaS	■
Kroll[1]	EMEA: Northern Europe; EMEA: Western Europe	Financial services Healthcare Professional services	On-premises Hosted, private SaaS Multitenant SaaS	■
Kudelski Security	EMEA: Northern Europe; EMEA: Western Europe	Financial services Manufacturing/production of consumer products Utilities	On-premises Hosted, private SaaS Multitenant SaaS	■
Kyndryl[1]	EMEA: Northern Europe; EMEA: Southern Europe	Financial services Insurance Manufacturing/production of industrial products	On-premises Hosted, private SaaS	■ ■
NCC Group	EMEA: Northern Europe; EMEA: Western Europe	Education and social services Financial services IT/tech services	On-premises Hosted, private SaaS Multitenant SaaS	■ ■
Obrela	EMEA: Middle East; EMEA: Northern Europe; EMEA: Southern Europe; EMEA: Western Europe	Construction and engineering Financial services Manufacturing/production of industrial products	On-premises Hosted, private SaaS Multitenant SaaS	■

Size ■ ■ ■ Large ≥$250M ■ ■ Medium $100M to <$250M ■ Small $10M to <$100M

Note: Geographic focus indicates regions where the provider's product revenue in this category is greater than or equal to 15% of its total product revenue.

1. The information about this provider includes Forrester's estimates.

Provider	Geographic focus	Industry focus	Type of partner	Size
Ontinue[1]	EMEA: Western Europe	Financial services Manufacturing/production of consumer products Manufacturing/production of industrial products	Multitenant SaaS	■
Orange Cyberdefense	EMEA: Northern Europe; EMEA: Western Europe	Financial services Healthcare Manufacturing/production of industrial products	On-premises Hosted, private SaaS Multitenant SaaS	■ ■
Palo Alto Networks[1]	EMEA: Western Europe	Education and social services Financial services Healthcare	Multitenant SaaS	■
Tata Consultancy Services	EMEA: Northern Europe; EMEA: Western Europe	Financial services Retail Transportation	On-premises Multitenant SaaS	■ ■
Telefónica Tech	EMEA: Southern Europe	Financial services Government Retail	Hosted, private SaaS Multitenant SaaS	■
Trend Micro	EMEA: Middle East; EMEA: Western Europe	Financial services Healthcare Manufacturing/production of high-tech products	Multitenant SaaS	■
Trustwave	EMEA: Middle East; EMEA: Northern Europe	Financial services Healthcare Professional services	On-premises Hosted, private SaaS Multitenant SaaS	■
WithSecure	EMEA: Northern Europe; EMEA: Western Europe	Financial services IT/tech services Manufacturing/production of high-tech products	Multitenant SaaS	■

Size ■ ■ ■ Large ≥$250M ■ ■ Medium $100M to <$250M ■ Small $10M to <$100M

Note: Geographic focus indicates regions where the provider's product revenue in this category is greater than or equal to 15% of its total product revenue.
1. The information about this provider includes Forrester's estimates.

Top Business Scenarios

We've identified the following core business scenarios for this market: detection, investigation, response, threat-hunting, and security posture improvement. These are the business scenarios that buyers most frequently seek and expect MDR service providers in Europe to address (see Figure 3). Beyond these core business scenarios, buyers often look for providers that focus on certain extended business scenarios. We've identified the following business scenarios as extended: detection engineering, vulnerability prioritization, managed security information and event management (SIEM), geographic threat contextualization, and deception technology (see Figure 4). Some buyers look to address these business scenarios in addition to the core ones, but MDR

service providers in Europe may less commonly address them.

Figure 3

Managed Detection And Response Services In Europe: Core Business Scenarios

Business scenario	Objective	Top differentiators
Detection	Use telemetry and signals to detect anomalous and unauthorized behavior	• Containers and workload detection • Software-as-a-service detection • Policy violations and misconfigurations
Investigation	Collect, analyze, and preserve forensic evidence to classify and determine best next steps during an incident	• Generative AI assistant • Federated search
Response	Guide and execute automated and manual actions on behalf of clients to contain, remediate, or recover from an incident	• Identity response • Automation and orchestration
Threat-hunting	Proactively detect adversarial activity via human-led, hypothesis-driven exercises	• Honeypots • Federated search
Security posture improvement	Provide proactive information to help security teams mature and harden their overall security posture	• Support for client-created detections • Policy violations and misconfigurations

Figure 4

Managed Detection And Response Services In Europe: Extended Business Scenarios

Business scenario	Objective	Top differentiators
Detection engineering	Build new detection rules	• Automation and orchestration • Support for client-created detections
Vulnerability prioritization	Provide context based on vulnerabilities to aid triage and remediation	• Generative AI assistant • Federated search
Managed SIEM	Manage the application layer of a SIEM platform to build queries, dashboards, and detections and run investigations	• Dashboard and report customization • Federated search
Geographic threat contextualization	Provide advisory and analysis based on geopolitical risk and region-specific adversarial tactics	• MITRE ATT&CK mapping
Deception technology	Provide decoys, traps and strategies to detect, study, and mislead adversaries	• Software-as-a-service detection • Containers and workload detection (Docker, Kubernetes)

Capability By Business Scenario

We've identified the 14 most important capabilities across the 10 most important business scenarios. Select the business scenarios that are most relevant to your business requirements and then use the following tables as a guide to choose the capabilities that matter most for your technology evaluation and provider selection criteria (see Figures 5 and 6).

Figure 5

Managed Detection And Response Services In Europe: Capability By Core Business Scenario

Capability	Detection	Investigation	Response	Threat-hunting	Security posture improvement
Standard detection (end-user compute, server, network, email)	●	●	●	○	○
Cloud detection (IaaS, PaaS, AWS, Azure, Google Cloud)	●	●	●	○	○
Containers and workload detection (Docker, Kubernetes)	●	●	●	○	○
Software-as-a-service detection	●	●	●	○	○
Response: common (endpoint, network)		○	●	○	
Identity response		○	●	○	
Automation and orchestration	●	●	●		○
Dashboard and report customization	●				
Generative AI assistant	●	●	○	○	
Federated search	○	●		○	○
MITRE ATT&CK mapping	○	○	○	○	●
Support for client-created detections	●			●	
Policy violations and misconfigurations	●		○	○	○
Honeypots	●	○		●	○

● **Primary capability** required for a given business scenario
○ **Secondary capability** required for a given business scenario
Little to no capability required for a given business scenario

Figure 6

Managed Detection And Response Services In Europe: Capability By Extended Business Scenario

Capability	Detection engineering	Vulnerability prioritization	Managed SIEM	Geographic threat contextualization	Deception technology
Standard detection (end-user compute, server, network, email)	●	○	○	◯	◯
Cloud detection (IaaS, PaaS, AWS, Azure, Google Cloud)	●	◯	○	◯	◯
Containers and workload detection (Docker, Kubernetes)	●	◯	○	◯	◯
Software-as-a-service detection	●	○	○	◯	◯
Response: common (endpoint, network)	○	●	◯	○	○
Identity response	○	◯	○	○	○
Automation and orchestration	◯	●	●	○	○
Dashboard and report customization	○	◯	●	○	○
Generative AI assistant	●	◯	○	◯	○
Federated search	●	◯	●	○	○
MITRE ATT&CK mapping	●	●	◯	◯	○
Support for client-created detections	●	◯	○	○	○
Policy violations and misconfigurations	◯	●	◯	◯	○
Honeypots	◯	●	◯	○	●

● **Primary capability** required for a given business scenario
◯ **Secondary capability** required for a given business scenario
○ **Little to no capability** required for a given business scenario

Provider Focus: Top Three Extended Business Scenarios

MDR service providers emphasize different aspects of their detection and response capabilities. Some providers emphasize capabilities like vulnerability prioritization, managed SIEM, and security posture improvement. We asked each participating provider in the report to select the top three extended business scenarios that it focuses on. These are three business scenarios, beyond the core ones, that the provider wants customers to recognize as its areas of focus (see Figure 7). This table doesn't represent available capabilities and may not represent the only business scenarios that providers serve.

Figure 7

Managed Detection And Response Services In Europe: Extended Business Scenario By Provider

Provider	Detection engineering	Vulnerability prioritization	Managed SIEM	Geographic threat contextualization	Deception technology
Bitdefender	✓	✓		✓	
BlueVoyant	✓	✓	✓		
CGI	✓		✓	✓	
CrowdStrike	✓		✓	✓	
CyberProof	✓	✓		✓	
Deutsche Telekom	✓	✓	✓		
eSentire	✓	✓		✓	
ESET	✓	✓	✓		
EY		✓	✓	✓	
HCLTech	✓		✓	✓	
I-TRACING	✓	✓	✓		
Kroll	✓		✓	✓	
Kudelski Security	✓		✓	✓	
Kyndryl	✓	✓	✓		
NCC Group	✓	✓	✓		

Note: The following provider declined to provide business scenario information in our questionnaire: Accenture.

Provider	Detection engineering	Vulnerability prioritization	Managed SIEM	Geographic threat contextualization	Deception technology
Obrela	✓	✓		✓	
Ontinue	✓	✓	✓		
Orange Cyberdefense	✓	✓	✓		
Palo Alto Networks	✓		✓	✓	
Tata Consultancy Services	✓	✓	✓		
Telefónica Tech		✓	✓	✓	
Trend Micro	✓	✓	✓		
Trustwave	✓	✓	✓		
WithSecure	✓	✓		✓	

Note: The following provider declined to provide business scenario information in our questionnaire: Accenture.

Supplemental Material

Methodology

To complete our review, Forrester requested information from providers. If providers didn't share this information with us, we made estimates based on available secondary information. We've marked all estimates with a note. Forrester shared a preview of this report with participating providers before publishing.

Companies We Researched For This Report

Forrester researched the following companies for this report.

Accenture

Bitdefender

BlueVoyant

CGI

CrowdStrike

CyberProof

Deutsche Telekom

eSentire

ESET

EY

HCLTech

I-TRACING

Kroll

Kudelski Security

Kyndryl

NCC Group

Obrela

Ontinue

Orange Cyberdefense

Palo Alto Networks

Tata Consultancy Services

Telefónica Tech

Trend Micro

Trustwave

WithSecure

FORRESTER®

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com