

# Managed Detection and Response (MDR) Services – Provider Compendium 2023

February 2023: Complimentary Abstract / Table of Contents



# Our research offerings

This report is included in the following research program(s):

## Cybersecurity

- ▶ Amazon Web Services (AWS)
- ▶ Application Services
- ▶ Artificial Intelligence (AI)
- ▶ Asset and Wealth Management
- ▶ Banking and Financial Services Business Process
- ▶ Banking and Financial Services Information Technology
- ▶ Catalyst™
- ▶ Clinical Development Technology
- ▶ Cloud and Infrastructure
- ▶ Contingent Staffing
- ▶ Contingent Workforce Management
- ▶ Customer Experience Management Services
- ▶ CX Excellence
- ▶ CXM Technology
- ▶ Cybersecurity
- ▶ Data and Analytics
- ▶ Digital Adoption Platforms
- ▶ Digital Engineering Services
- ▶ Digital Services
- ▶ Digital Workplace
- ▶ Employee Experience Management (EXM) Platforms
- ▶ Employer of Record (EOR)
- ▶ Engineering Services
- ▶ Enterprise Platform Services
- ▶ Exponential Technologies
- ▶ Finance and Accounting
- ▶ Financial Services Technology (FinTech)
- ▶ GBS Talent Excellence
- ▶ Global Business Services
- ▶ Google Cloud
- ▶ Healthcare Business Process
- ▶ Healthcare Information Technology
- ▶ Human Resources
- ▶ Insurance Business Process
- ▶ Insurance Information Technology
- ▶ Insurance Technology (InsurTech)
- ▶ Insurance Third-Party Administration (TPA) Services
- ▶ Intelligent Document Processing
- ▶ Interactive Experience (IX) Services
- ▶ IT Services Excellence
- ▶ IT Services Executive Insights™
- ▶ IT Talent Excellence
- ▶ Life Sciences Business Process
- ▶ Life Sciences Commercial Technologies
- ▶ Life Sciences Information Technology
- ▶ Locations Insider™
- ▶ Marketing Services
- ▶ Market Vista™
- ▶ Microsoft Azure
- ▶ Modern Application Development (MAD)
- ▶ Mortgage Operations
- ▶ Multi-country Payroll
- ▶ Network Services and 5G
- ▶ Oracle Services
- ▶ Outsourcing Excellence
- ▶ Pricing Analytics as a Service
- ▶ Process Mining
- ▶ Process Orchestration
- ▶ Procurement and Supply Chain
- ▶ Recruitment
- ▶ Retail and CPG Information Technology
- ▶ Retirement Technologies
- ▶ Revenue Cycle Management
- ▶ Rewards and Recognition
- ▶ SAP Services
- ▶ Service Optimization Technologies
- ▶ Software Product Engineering Services
- ▶ Supply Chain Management (SCM) Services
- ▶ Sustainability Technology and Services
- ▶ Technology Skills and Talent
- ▶ Trust and Safety
- ▶ Value and Quality Assurance (VQA)
- ▶ Work at Home Agent (WAHA) Customer Experience Management (CXM)

If you want to learn whether your organization has a membership agreement or request information on pricing and membership options, please contact us at [info@everestgrp.com](mailto:info@everestgrp.com)

Learn more about our  
**custom research capabilities**

Benchmarking

Contract assessment

Peer analysis

Market intelligence

Tracking: providers, locations,  
risk, technologies

Locations: costs, skills,  
sustainability, portfolios

# Contents

<b>1. Introduction and overview</b>	<b>5</b>
• Research methodology	6
• Key information on the report	7
• Background of research	8
• Focus of the research	9
<b>2. Managed Detection &amp; Response (MDR) Services PEAK Matrix® Characteristics</b>	<b>10</b>
• PEAK Matrix framework	11
• Managed Detection and Response (MDR) Service PEAK Matrix Assessment	13
• Characteristics of Leaders, Major Contenders, and Aspirants	14
• Service provider capability summary dashboard	15
<b>3. Enterprise sourcing consideration</b>	<b>19</b>
• Leaders	19
– Accenture	20
– Atos	27
– HCLTech	33
– IBM	39
– Orange Cyberdefense	45
– TCS	51
– Wipro	57
• Major Contenders	63
– Capgemini	64
– Cognizant	70
– Cyberproof	76

For more information on this and other research published by Everest Group, please contact us:

**Kumar Avijit**, Practice Director

**Arjun Chauhan**, Senior Analyst

**Malsawmkima Sailung**, Senior Analyst

# Contents

● Major Contenders (continued)	
– Deloitte	82
– DXC Technology	88
– FIS Global	94
– Happiest Minds	100
– Infosys	106
– Kyndryl	112
– LTI	118
– Microland	124
– NTT DATA	131
– Tech Mahindra	138
– T-Systems	144
– Zensar	150
● Aspirants	156
– GAVS Technologies	157
– Mindtree	163
– Mphasis	169
– Stefanini	175
– Tata Communications	181
<b>5. Appendix</b>	<b>187</b>
● Glossary	188
● Research calendar	189

# 01

---

## Introduction and overview

- Research methodology

---

- Key information on the report

---

- Introduction

---

- Focus of the research

## Our research methodology is based on four pillars of strength to produce actionable and insightful research for the industry

01

### Robust definitions and frameworks

Function specific pyramid, Total Value Equation (TVE), PEAK Matrix®, and market maturity

02

### Primary sources of information

Annual contractual and operational RFIs, provider briefings and buyer interviews, web-based surveys

03

### Diverse set of market touchpoints

Ongoing interactions across key stakeholders, input from a mix of perspectives and interests, supports both data analysis and thought leadership

04

### Fact-based research

Data-driven analysis with expert perspectives, trend-analysis across market adoption, contracting, and providers

Proprietary contractual database of over 300+ cybersecurity contracts (updated annually)

Year-round tracking of 30+ MDR service providers

Large repository of existing research in cybersecurity

Over 30 years of experience advising clients on strategic IT, business services, engineering services, and sourcing

Executive-level relationships with buyers, providers, technology providers, and industry associations

## This report is based on multiple sources of proprietary information

- Proprietary database of IT services contracts of major IT providers with workplace services in scope of work (updated annually)
- The database tracks the following elements of each contract:
  - Buyer details including size and signing region
  - Contract details including provider, contract type, TCV & ACV, provider FTEs, start & end dates, duration, and delivery locations
  - Scope details including share of individual buyer locations being served in each contract, Line of Business (LoB) served, and pricing model employed
- Proprietary database of IT providers (updated annually)
- The database tracks the following for each provider:
  - Revenue and number of FTEs
  - Number of clients
  - FTE split by different LoBs
  - Revenue split by region
  - Location and size of delivery centers
  - Technology solutions developed
- Provider briefings
  - Vision and strategy
  - Annual performance and future outlook
  - Key strengths and improvement areas
  - Emerging areas of investment
- Buyer reference interviews, ongoing buyer surveys, and interactions
  - Drivers and challenges for adopting workplace services
  - Assessment of provider performance
  - Emerging priorities
  - Lessons learned and best practices adopted

### Providers assessed<sup>1</sup>



<sup>1</sup> Analysis for LTI and Mindtree is based on capabilities before their merger

Note: **The source of all content is Everest Group unless otherwise specified**

Confidentiality: Everest Group takes its confidentiality pledge very seriously. Any information we collect that is contract specific will only be presented back to the industry in an aggregated fashion

## Introduction

Organizations are leveraging Managed Detection and Response (MDR) to improve their security operations, tackle and combat any known/unknown threats through the use of advanced technologies, and to preemptively mitigate attacks that can bring down the organization or create the possibility of having to pay heavy fines. The propensity of working from home increases the security challenges due to exposure to more vulnerabilities and creates an avenue for novel threats. As a result, it is humanly impossible to monitor and manage the increased alerts from the all-new technologies and devices as the organization expands its network. This, coupled with a shortage of cybersecurity talent, adds to their challenges. To bridge this gap, MDR enhances an organization's security posture through continuous monitoring, threat detection, and incident response underpinned by playbooks, verticalized SOCs, and expert talent. MDR services provide organizations with an effective response mechanism for known or unknown threats by mapping dynamic threat intelligence to the organization's assets.

In this research, we present an assessment and detailed profiles of 27 MDR service providers featured on the Managed Detection and Response (MDR) Services PEAK Matrix® Assessment. Each provider profile provides a comprehensive picture of its strengths and limitations. The assessment is based on Everest Group's annual RFI process for calendar year 2022, interactions with leading MDR service providers, client reference checks, and an ongoing analysis of the MDR services market.

**This report includes the profiles of the following 27 leading MDR providers featured on the [Managed Detection and Response \(MDR\) Services PEAK Matrix® Assessment 2023](#):**

- **Leaders:** Accenture, Atos, HCLTech, IBM, Orange Cyberdefense, TCS, and Wipro
- **Major Contenders:** Capgemini, Cognizant, CyberProof, Deloitte, DXC Technology, FIS Global, Happiest Minds, Infosys, Kyndryl, LTI, Microland, NTT DATA, Tech Mahindra, T-Systems, and Zensar
- **Aspirants:** GAVS Technologies, Mindtree, Mphasis, Stefanini, and Tata Communication

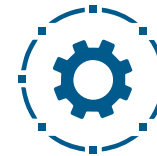
### Scope of this report



**Geography**  
Global



**Providers**  
27



**Services**  
Managed Detection and  
Response



# The Managed Detection and Response (MDR) Services report has over 27 provider profiles/buyer case studies/architecture of the survey questionnaire, etc.

Managed Detection and Response (MDR) Services – Provider Compendium 2023

## Provider | MDR services profile (page 1 of 6)

### Overview

**Company mission/vision statement**  
 Provider' MDR objective is to become one of the top from new and developing cyber threats. Provider is customer-centric approach to delivering services.

**MDR services revenue (2021)**

Retail, distribution, and CPG	High
Travel and transport	Medium

**Large revenue > US\$5 billion**  
 (annual revenue > US\$5 billion)

**Medium (15-40%)**  
 High (>40%)

**Geographic distribution**

World	High
Latin America	Medium

Managed Detection and Response (MDR) Services – Provider Compendium 2023

## Provider | MDR services profile (page 2 of 6)

### Case studies

**Case study 1** Threat response time move

**Client:** a global banking institution

**Business challenge**  
 In long attacker dwell times and damaging

With its MDR service delivered from Provider d sophisticated threats, and advanced threat worked with the client to contain identified ment for evicting the attacker.

Enhance threat detection and response and

Managed Detection and Response (MDR) Services – Provider Compendium 2023

## Provider | MDR services profile (page 3 of 6)

### Solutions

**Proprietary solutions (representative list)**

Solution name	Detail
MDR for Automotive	The M vehicle

Managed Detection and Response (MDR) Services – Provider Compendium 2023

## Provider | MDR services profile (page 4 of 6)

### Partnerships

**Partnerships (representative list)**

Partner name	Type of partnership
Partner 1	MDR partnership

Managed Detection and Response (MDR) Services – Provider Compendium 2023

## Provider | MDR services profile (page 5 of 6)

### Investments and recent ac

**Investments and recent activities (representative list)**

Themes	Details
Acquisition	Provider acquired ABC AI capabilities, and bring

Managed Detection and Response (MDR) Services – Provider Compendium 2023

## Provider | MDR services profile (page 6 of 6)

### Everest Group assessment – Leader

Measure of capability: ● Low ● High

Market impact			Vision & capability					
Market adoption	Portfolio mix	Value delivered	Overall	Vision and strategy	Scope of services offered	Innovation and investments	Delivery footprint	Overall
<span style="color: blue;">●</span>	<span style="color: blue;">●</span>	<span style="color: blue;">●</span>	<span style="color: blue;">●</span>	<span style="color: blue;">●</span>	<span style="color: blue;">●</span>	<span style="color: red;">●</span>	<span style="color: blue;">●</span>	<span style="color: red;">●</span>

**Strengths**

- Enterprise buyers looking for advanced threat hunting can consider Provider for its automated threat hunting capabilities, which are backed by 100+ ML models and 200+ threat intel sources
- Provider will be a relevant choice for enterprises looking to engage in consulting and operational MDR services. It recently acquired ABC, DEF, and HIJ to strengthen its cybersecurity talent across different regions
- European enterprises with data sovereignty requirements can leverage the Sovereign MDR offering by Provider coupled with its six localized SOCs in the EU

**Limitations**

- Enterprises looking for cost-competitive service Provider as its delivery mix is more onshore-focus offer price discounts compared to peers
- Some clients have highlighted that Provider lags pe OT/ICS sources
- Enterprises might need to validate the cohesiveness and ABC split completion

Buyers looking for industrial SOCs will find Provider attractive because of its large use-case library and industry-specific offerings in automotive, media, and healthcare verticals

Enterprise buyers looking for add-on MDR capabilities can evaluate Provider' offerings such as data forensics, vulnerability management, external attack surface management, penetration testing, device management, and red teaming

6 Everest Group® Proprietary & Confidential. © 2023, Everest Global, Inc. | EGR-2023-65-R-5856

# Research calendar

## Cybersecurity

Published Planned Current release

Reports title	Release date
Supplier Management Toolkit: Cybersecurity Risk Management in the Supplier Life Cycle	January 2022
Getting to the Bottom of Zero Trust (ZT) Security	April 2022
Technology Vendor Snapshot for OT Security	June 2022
IT Security Services PEAK Matrix® Assessment 2022 – North America	July 2022
IT Security Services PEAK Matrix® Assessment 2022: Europe	August 2022
IT Security Services Provider Compendium 2022 – North America	September 2022
IT Security Services Provider Compendium 2022 – Europe	September 2022
Managed Detection and Response (MDR) Services PEAK Matrix® Assessment 2023	December 2022
<b>Managed Detection and Response (MDR) Services – Provider Compendium 2023</b>	<b>February 2023</b>
Managed Detection and Response (MDR) State of the Market 2023	Q1 2023
IT Security Services State of the Market 2023	Q1 2023
Data Security and Privacy	Q2 2023
Technology Vendor Snapshot for IAM	Q2 2023

Note: [Click](#) to see a list of all of our published Cybersecurity reports



Everest Group is a leading research firm helping business leaders make confident decisions. We guide clients through today's market challenges and strengthen their strategies by applying contextualized problem-solving to their unique situations. This drives maximized operational and financial performance and transformative experiences. Our deep expertise and tenacious research focused on technology, business processes, and engineering through the lenses of talent, sustainability, and sourcing delivers precise and action-oriented guidance. Find further details and in-depth content at [www.everestgrp.com](http://www.everestgrp.com).

## Stay connected

### Website

[everestgrp.com](http://everestgrp.com)

### Social Media

 [@EverestGroup](https://twitter.com/EverestGroup)

 [@Everest Group](https://www.linkedin.com/company/everestgrp)

 [@Everest Group](https://www.facebook.com/EverestGroup)

 [@Everest Group](https://www.youtube.com/EverestGroup)

### Blog

[everestgrp.com/blog](http://everestgrp.com/blog)

### Dallas (Headquarters)

[info@everestgrp.com](mailto:info@everestgrp.com)

+1-214-451-3000

### Bangalore

[india@everestgrp.com](mailto:india@everestgrp.com)

+91-80-61463500

### Delhi

[india@everestgrp.com](mailto:india@everestgrp.com)

+91-124-496-1000

### London

[unitedkingdom@everestgrp.com](mailto:unitedkingdom@everestgrp.com)

+44-207-129-1318

### Toronto

[canada@everestgrp.com](mailto:canada@everestgrp.com)

+1-416-388-6765

This document is for informational purposes only, and it is being provided "as is" and "as available" without any warranty of any kind, including any warranties of completeness, adequacy, or fitness for a particular purpose. Everest Group is not a legal or investment adviser; the contents of this document should not be construed as legal, tax, or investment advice. This document should not be used as a substitute for consultation with professional advisors, and Everest Group disclaims liability for any actions or decisions not to act that are taken as a result of any material in this publication.