



# Everest Group Managed Detection and Response (MDR) Services PEAK Matrix<sup>®</sup> Assessment 2025

Focus on Accenture

March 2025



# Introduction

As organizations face an expanding attack surface due to the proliferation of cloud computing, Internet of Things (IoT) devices, and convergence of Information Technology (IT) and Operational Technology (OT), they are increasingly relying on MDR providers to navigate these complexities by offering real-time visibility across interconnected systems, rapid containment of sophisticated threats, and seamless integration with existing security frameworks. Key challenges for enterprises include managing complex security environments, addressing talent shortages while facing budget constraints.

Service providers are addressing these needs by integrating cutting-edge innovations such as gen AI for threat detection, SOC-as-a-service for flexible, cloud-based operations, and Extended Detection and Response (XDR) capabilities to provide comprehensive telemetry coverage. Additionally, the convergence of IT and OT environments has driven the need for unified Security Operation Centers (SOCs) capable of managing diverse and interconnected ecosystems.

In the research, we present an assessment and detailed profiles of 29 MDR service providers from around the globe, featured on the [Managed Detection and Respond \(MDR\) Services PEAK Matrix® Assessment 2025](#). The assessment is based on Everest Group's annual RFI process for the calendar year 2024, interactions with leading MDR service providers, client reference checks, and ongoing analysis of the MDR services market.

**The full report includes the profiles of the following 29 leading MDR Service providers featured on the Managed Detection and Respond (MDR) Services PEAK Matrix 2025:**

- **Leaders:** Accenture, Deloitte, Eviden, HCLTech, IBM, NTT DATA, TCS, and Wipro
- **Major Contenders:** Capgemini, Cognizant, CyberProof, DXC Technology, EY, Infosys, Inspira, Kudelski Security, Kyndryl, LevelBlue, LTIMindtree, Optiv, Orange Cyberdefense, Tata Communications, Tech Mahindra, and Telefonica
- **Aspirants:** Birlasoft, Happiest Minds, Persistent Systems, Stefanini, and Zensar

## Scope of this report

**Geography:** global

**Industry:** all-encompassing industries globally

**Services:** MDR

**Use cases:** we have only analyzed publicly available information (~90 distinct use cases) in this report

# Managed Detection and Response (MDR) services PEAK Matrix® characteristics

## Leaders

Accenture, Deloitte, Eviden, HCLTech, IBM, NTT DATA, TCS, and Wipro

- Leaders in the MDR market demonstrate a robust ability to meet the diverse and evolving needs of enterprises by delivering end-to-end MDR services. They maintain strong capabilities in integrating advanced technologies such as gen AI, XDR, and IT-OT security convergence to provide proactive threat detection, automated incident response, and seamless security operations
- Leaders also exhibit a strong focus on co-innovation through a well-developed ecosystem of partnerships with leading technology providers. Their comprehensive offerings ensure wide market impact, consistent YoY growth, and trust among enterprises navigating sophisticated cyber threats

## Major Contenders

Capgemini, Cognizant, CyberProof, DXC Technology, EY, Infosys, Inspira, Kudelski Security, Kyndryl, LevelBlue, LTIMindtree, Optiv, Orange Cyberdefense, Tata Communications, Tech Mahindra, and Telefonica

- Major Contenders are steadily increasing their market presence in the MDR segment by expanding service portfolios and investing in IP and accelerators to enhance their detection and response capabilities. They effectively leverage partnerships with top technology vendors to deliver value-added services such as SOC-as-a-service and flexible pricing options
- While these providers offer strong capabilities in select MDR areas, they often lag leaders in delivering holistic solutions and achieving a wide market impact. Their focus on innovation and targeted growth positions them as formidable competitors in the MDR landscape

## Aspirants

Birlasoft, Happiest Minds, Persistent Systems, Stefanini, and Zensar

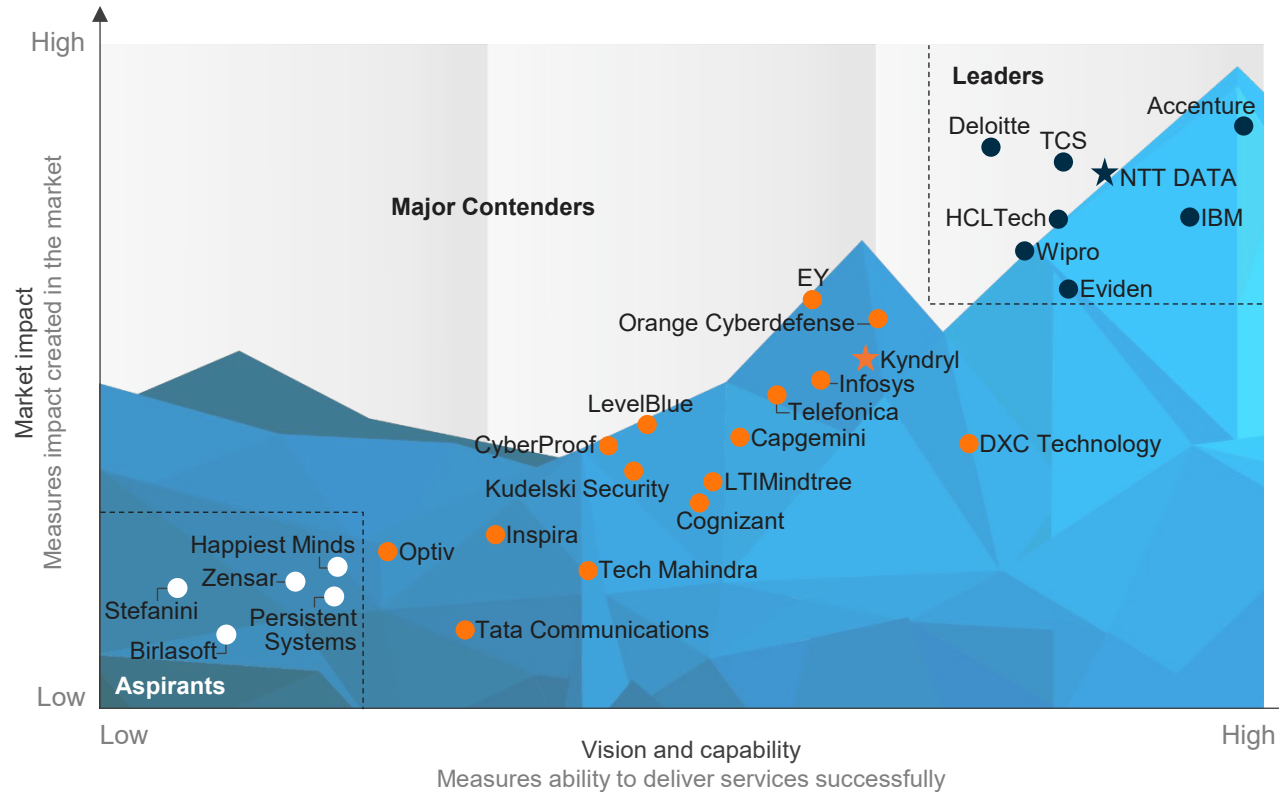
- Aspirants in the MDR market operate in niche areas and focus on addressing specific client needs, typically in small and mid-market segments
- These providers are in the early stages of developing their MDR capabilities and lack the scale to cater to large or global clients effectively
- Despite their narrower service scope, Aspirants are actively building capabilities through investments in proprietary IP, workforce development, and targeted service enhancements. Their focus on specialized segments positions them as emerging players with potential for growth in the MDR space

# Everest Group PEAK Matrix®

Managed Detection and Response (MDR) Services PEAK Matrix® Assessment 2025 | Accenture is positioned as a Leader

## Everest Group Managed Detection and Response (MDR) Services PEAK Matrix® Assessment 2025<sup>1</sup>

- Leaders
- Major Contenders
- Aspirants
- ☆ Star Performers



<sup>1</sup> Assessments for Tech Mahindra, Deloitte, Eviden, EY, and LevelBlue excludes service provider inputs and are based on Everest Group's proprietary Transaction Intelligence (TI) database, provider public disclosures, and Everest Group's interactions with buyers. 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 be presented only in an aggregated fashion.

# Accenture profile (page 1 of 7)

## Overview

### Company mission/vision statement

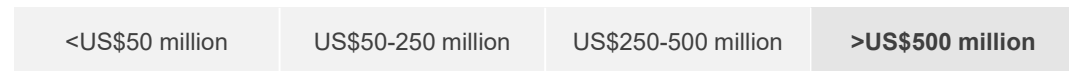
Accenture’s vision is to empower clients to confidently detect and respond to cyber events through four key principles: Adaptability, Innovation, Delivery Excellence, and One Global Accenture. Adaptability offers flexible, end-to-end solutions that evolve with client scenarios by integrating advanced technologies and proprietary assets for comprehensive coverage across IT, OT, and IoT, tailored to specific industry and regional needs.

Innovation uses the Industry Content Library, automation, and gen AI to rapidly develop and deploy capabilities for effective detection, investigation, and response, while ensuring smooth transitions between platforms.

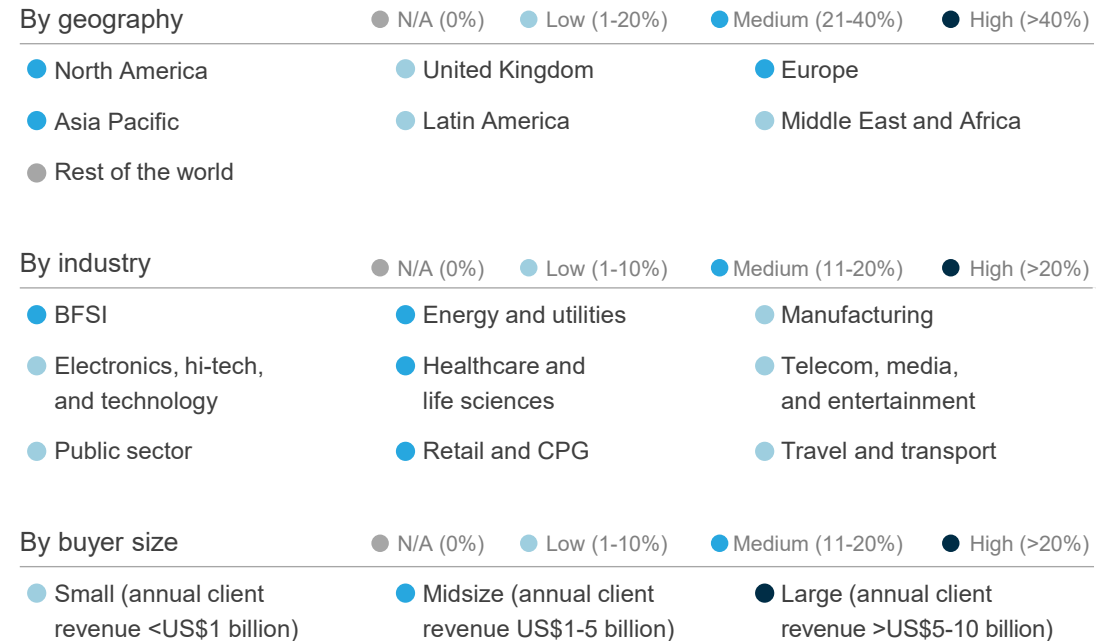
Delivery Excellence focuses on global consistency, offering trusted, round-the-clock support, timely insights, and continuous improvement through rigorous quality controls and feedback, building reliable long-term partnerships.

One Global Accenture reflects a collaborative approach, leveraging the expertise of 774,000 employees to deliver comprehensive cybersecurity services across industries and geographies, enhanced by innovative technologies to meet evolving challenges.

### Overall MDR services revenue (CY 2023)



### MDR services revenue mix (CY 2023)



# Accenture profile (page 2 of 7)

## Case studies

### CASE STUDY 1

Continuous evolution of IT and OT security capabilities to maintain pace with cyber threats faced by the US electric grid

**Client:** US west electric utility company

#### Business challenge

- The client had limited OT security program capabilities across protect, detect, respond, and govern
- The client was seeking expert advisory to craft enterprise and grid network security monitoring including key technology solutions, 24x7 coverage, and purple team operations

#### Solution and impact

- Expanded SOAR capabilities across enterprise and grid networks to achieve enrichment, prioritization, and automated response
- Established the OT security program strategy including risk management, cross-functional governance model, asset management integration, security tool optimization, and continuous security monitoring use cases
- Delivered 40+ security architecture, engineering, and risk assessments for IT and OT technology solutions, ensuring a comprehensive view
- Designed, implemented, and trained OT security operations staff to augment grid monitoring and achieve 24x7 NOC and SOC coverage
- Implemented ServiceNow SecOps, Governance, Risk, and Compliance (GRC), and Strategic Portfolio Management (SPM) for improved operations and governance across the enterprise
- Conducted penetration testing and red team operations for the grid network including transmission operations and field area networks

#### Key benefits

- Expert cyber advisory: helped the client optimize its SIEM, SOAR, and GRC solutions
- Continuous transformation: implemented and extended key platforms including SOAR and vulnerability management, creating a complete life cycle of cyber threat and vulnerability detection, prioritization, and response resulting in a 30% Mean Time To Respond (MTTR) improvement and accelerated vulnerability response
- Cyber risk and impact reduction: Accenture's security architecture, engineering, and risk assessment services enabled security by design in new technology solutions (built and bought), enabled by the implementation of ServiceNow GRC for cyber risk management, SecOps for SOC workflow, and SPM for managing the security solution fleet

### CASE STUDY 2

Fully managed IT/OT SOC service based on Microsoft Sentinel SIEM and Google Chronicle SOAR

**Client:** European consumer goods company

#### Business challenge

The client was dissatisfied with its cybersecurity providers and sought to consolidate OT and IT detection and response under a single strategic partner within a managed SOC. As a heavily outsourced enterprise, it required a strong and strategic security partnership. Both the SOC platform and services, including the operating model, needed a refresh, prompting the client to seek a partner for a multi-year transformation journey. Key selection criteria included the partner's maturity to support long-term enterprise growth and its ability to drive innovation. Accenture's Hybrid MxDR on Microsoft Sentinel emerged as the ideal solution.

#### Solution and impact

- Accenture leverages both Google Gemini gen AI and its own operational gen AI for report generation, language translation, malware investigation, and other use cases
- Advanced cybersecurity services, including threat hunting and cyber threat intelligence, integrated into the SOC service and joined up with the client's internal teams
- Incident response retainer service to cover both IT and OT environments
- Accenture services encompass 24/7 security monitoring of the client's full IT/OT environments in all countries, powered by Accenture, Mandiant, and VirusTotal threat intelligence
- Service integrated into the existing tech stack including ITSM, change management, and agile delivery

#### Key benefits

- Delivered Hybrid-MxDR solution based on Sentinel SIEM and Google Chronicle SOAR architecture, competitive in cost and innovative in capabilities
- Leveraged Accenture's accelerators and experience in conducting complex transitions and transformations with the agile model, minimizing operational risk to the client
- Measures for automation (for example, Chronicle SOAR) and threat intelligence, enabling operational playbooks and use cases for the client's industry
- 45 OT sites onboarded, with 30k+ OT assets monitored via Claroty xDome and a very low number of false positives
- CIO-level reporting measuring service value with improved security posture and risk reduction

# Accenture profile (page 3 of 7)

## Solutions

[REPRESENTATIVE LIST]

### Proprietary MDR services solutions

Solution	Details
Industry Content Library	The Industry Content Library is a central pillar of the Accenture Adaptive Detection and Response Strategy, built on extensive experience in developing, transforming, and operating SOCs for over 800 clients. It is a comprehensive and continuously evolving repository of detection use cases, playbooks, reports, dashboards, and threat hunting models, organized by industry, domain, and topic. The library is used by 1,400+ experts in Accenture's MDR team, leveraging and contributing to it every day. This includes Accenture's Content Factory team of 100+ engineers developing and tailoring new content around the clock for clients and some key partners (outsourcing to Accenture the development of their products' dashboards, out-of-the-box collectors, detections, etc.).
Adaptive MxDR Portal	Leveraging its years of experience with a client front-end portal, Accenture launched a new Adaptive MxDR Portal to maximize the value of its services for its clients. It provides enhanced user experience for all aspects of the MxDR service, with integrated access to both the Accenture platform and the clients' platforms augmented by gen AI functionality (including language translation). This provides clients with full access into the platform, configurations, policies, and data, avoiding any black-box concerns. The customizable homepage is role-based offering different views based on the user's role and responsibilities (for example, CISO versus SOC analyst).
Threat Intel	Accenture emphasizes an intelligence-led approach across its security offerings. With Adaptive MxDR, Accenture leverages its front-line knowledge of the threat landscape as well as insights from leading ecosystem partnerships to contextualize the threats that matter most for clients. Accenture's approach offers a flexible model that operationalizes intelligence across a range of client needs, allowing it to contextualize this data in the context of the client's business and industry. Accenture's capabilities range from basic orchestration enhancement and automation to more advanced services that can drive proactive threat hunting, enterprise risk management, and strategic planning. Accenture's data holdings include over 25 years of threat context and integrate feeds from over 60 providers (including Google, Mandiant, and VirusTotal) to enhance its ability to detect and respond to threats.
Operational gen AI	Through the co-development with clients of Accenture's Security AI Assistant capability (an Accenture IP), it developed a standardized approach, platform, and gen AI development pipeline using a use case-based approach that moved from design and build to production ready capabilities in early 2024. Then in 2024, with a baseline set of use cases in production across all MDR services (as defined in the provided market definition), Accenture shifted to a more holistic approach to focus not just on use cases, but more on developing end-to-end capabilities aligned with tangible outcomes for its clients.

# Accenture profile (page 4 of 7)

## Partnerships

[REPRESENTATIVE LIST]

### Partnerships

Partner	Type of partnership	Details
Google + Mandiant	Technology and service partnership	Accenture partners with Google to deliver MDR services leveraging the Google SecOps suite, which includes close collaboration with Google Engineering and exclusive access to Google AI models (Gemini, Sec-PaLM). Accenture also works with Google to develop their dashboarding with the product set. Announced in May 2024, Accenture and Mandiant, part of Google Cloud, are teaming up to deliver cyber resilience services to help organizations more efficiently detect, investigate, respond to, and recover from cyberattacks, using Mandiant as a key threat intelligence source
Microsoft	Technology partnership	Accenture partners with Microsoft on the Azure Security technology offerings to deliver MDR services to its clients. This includes close collaboration with Microsoft Engineering and a pre-built library of use cases, numerous Accenture engineers and clients contributing. Accenture is proud to be the 2024 Microsoft SI Partner of the Year (for 19 consecutive years).
Splunk	Technology partnership	Accenture partners with Splunk on technology offerings to deliver MDR services to its clients. This includes accelerators such as the pre-built use-case library, with numerous Accenture engineers contributing.
CrowdStrike	Technology partnership	Accenture partners with CrowdStrike across its 28 different modules (at the time of writing) spanning cloud, identity, endpoint, and SIEM. Accenture was awarded the 2024 Emerging GSI Partner of the Year, highlighting the considerable strides both parties have made, since committing to the partnership.
Palo Alto Networks	Technology partnership	Accenture and Palo Alto Networks expanded their strategic alliance to integrate Palo Alto's Precision AI™ technology with Accenture's secure gen AI services. This initiative aims to enhance cybersecurity capabilities, especially in the context of AI transformation journeys for enterprises.
Nozomi Networks	Technology partnership	Accenture's detection and response team is a participant in Nozomi Networks' new Elite Cyber Defenders Program. The program enables leading global incident response enterprises with Nozomi Networks' OT and IoT cybersecurity solutions, advanced security training, shared threat intelligence, and joint security research. The team utilizes Nozomi for all incidents – more broadly, Accenture partners with Nozomi for secure connected devices (IoT/IIoT/ICS) and embedded systems to enable intelligent, connected, and trusted products and services for its clients to use internally and to sell to their customers.
Immersive Labs	Service partnership	Accenture and Immersive Labs partnered to launch Cyber Million, a program dedicated to filling one million entry-level cybersecurity operations jobs over the next decade.
Rubrik	Technology partnership	Accenture works collaboratively with Rubrik to deliver enhanced secure backup solutions and architecture focused on response and reduced recovery times.



# Accenture profile (page 5 of 7)

## Investments and recent activities

[REPRESENTATIVE LIST]

### Investments and recent activities

Themes	Details
Acquisitions	Invested in acquisitions to expand MDR services including Innotec (Spain, Novemeber 2023), MNEMO (Mexico, October 2023), Morphus (Brazil, February 2023), and ARZ (Austria, December 2022)
Talent	<ul style="list-style-type: none"> <li>• Accenture has built talent forecasting tools to anticipate demand across dimensions such as experience level, skill, location, and more, to ensure it delivers quality client experiences</li> <li>• Accenture has invested in and partnered with Immersive Labs to help members of its cyber resilience team create a career framework by giving them the skills and tools necessary to chart their careers</li> <li>• For talent retention, Accenture has a cross-training and mentorship program to provide its security practitioners across various domains the ability to transition across cybersecurity teams</li> <li>• Accenture is committed to ensuring it has a diverse range of backgrounds, and equality of representation, regardless of gender, disability, ethnic, and racial background</li> </ul>
R&D and innovation	<ul style="list-style-type: none"> <li>• Adaptive MxDR service: multimillion-dollar investment to move from legacy, proprietary service to a new adaptive service based on an open, extensible platform leveraging all the new functions described above such as the new portal, content library, gen AI, integrated Google SecOps, and integrated additional intel feeds (for example, Mandiant)</li> <li>• Gen AI: Accenture has invested US\$3 billion to date in gen AI over three years and Adaptive MxDR has used some of that investment to enhance the new offering</li> <li>• Geo-aware programs: Accenture has invested in country-specific platforms for MxDR, including an EU-only platform that can only be accessed within the EU, and a similar one exclusively for the US</li> <li>• Accenture's incident response capabilities include bespoke tooling and proprietary playbooks for rebuilding diverse environments and custom OT collection tools. Key investment areas include digitizing crisis management Day 1 asset, enhancing global training consistency through its partnership with Immersive Labs, leveraging gen AI for security AI assistant, and developing a data processing tool that delivers fast client insights</li> <li>• SOC transformation offering to enable the future of security operations: It evolves security operations center capabilities to enable the capture of core transformation initiatives such as a talent development plan, the convergence of tools and platforms, data transformation, scalable automation, gen AI, and engineering-driven operations</li> <li>• Demo environments to showcase data and infrastructure resilience with key partners: scale client engagement through solution showcases tailored to common client and industry security challenges and solved through proprietary solutions</li> <li>• Extend Continuous Threat Exposure Management (CTEM) offering for market shifts: redesigns traditional TEM services to be a vertically integrated managed service capability, enabling a broader set of capabilities and better outcomes for clients</li> </ul>

# Accenture profile (page 6 of 7)

## Investments and recent activities

[REPRESENTATIVE LIST]

### Investments and recent activities

Themes	Details
MDR start-up ecosystem	<ul style="list-style-type: none"> <li>• Clarity: The system provides monitoring and anomaly detection, employing models and algorithms to alert customers to both cybersecurity and process integrity issues</li> <li>• Endgame (now part of Elastic): Endgame provides threat hunting services, incident response services, and security operations managed services</li> <li>• InCountry: InCountry's Data Residency-as-a-Service (DRaaS) platform enables enterprises and Software-as-a-Service (SaaS) companies to ensure their company and customer data is used in compliance with the data residency regulations of 90+ countries and has become an urgent imperative for Accenture's enterprise clients</li> <li>• Interos: The Interos platform uses AI and machine learning to monitor and analyze a wide array of supply chain issues in real time across financial, operational, governance, geographic, and cybersecurity</li> <li>• Ripjar: To better serve clients, Accenture leverages Ripjar's technology by building dedicated modules on top of their flexible and powerful platform</li> <li>• Symmetry Systems: Symmetry Systems offers data store and object-level security (DSOS) solutions that give organizations visibility into, and unified access control of, their most valuable data assets</li> <li>• Team8: Team8 works hand-in-hand with entrepreneurs to build successful companies that can transform the cybersecurity paradigm; its unique company ideation and creation environment provides the building blocks to create disruptive, industry-leading cybersecurity companies</li> </ul>










# Accenture profile (page 7 of 7)

Everest Group assessment – Leader

Measure of capability:  Low  High

## Market impact

## Vision and capability

Market impact				Vision and capability				
Market adoption	Portfolio mix	Value delivered	Overall	Vision and strategy	Scope of services offered	Innovation and investments	Delivery footprint	Overall
								

### Strengths

- Enterprises seeking global reach and scalability benefit from Accenture's extensive network of 22 centers and over 4,000 MDR professionals
- Enterprises with developing security programs can leverage Accenture's tiered pricing model, beginning with a basic level of MDR services and scaling up gradually as their requirements expand
- Enterprises seeking operational resilience can leverage Accenture's Cyber Operational Resilience (CORE) framework, which enhances and operationalizes MITRE ATT&CK for improved detection and response
- Enterprises seeking modular MDR solutions benefit from Accenture's flexible platform options, including full-stack and hybrid deployment, seamlessly supporting multi-vendor and client-owned ecosystems
- Enterprises seeking gen AI-led MDR service can benefit from Accenture's advanced security operations, automating tasks, enhancing threat hunting, and optimizing security for increased efficiency and faster response

### Limitations

- Accenture's focus on large-scale, complex projects and enterprise clients may not align well with the needs of small scale enterprises, which often require more cost-effective solutions
- Clients have expressed concerns about the lack of visibility into resource utilization and performance metrics, making it difficult to assess the value and cost-effectiveness of services
- Clients have indicated a need for more innovative thinking and efficient investigation procedures from Accenture's offshore team to improve problem-solving and overall service delivery
- Enterprises requiring flexible contract durations may face constraints with Accenture's standard minimum three-year deal tenure requirement

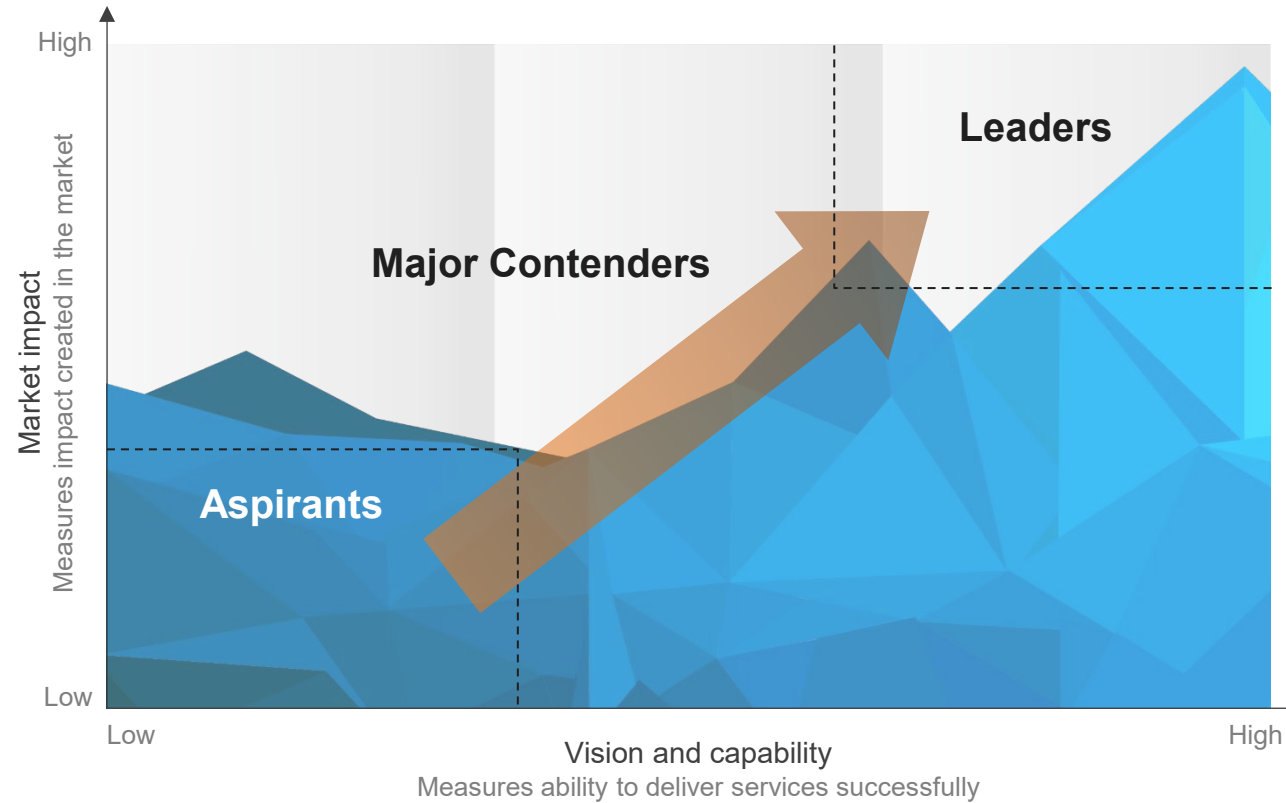
# Appendix

PEAK Matrix® framework

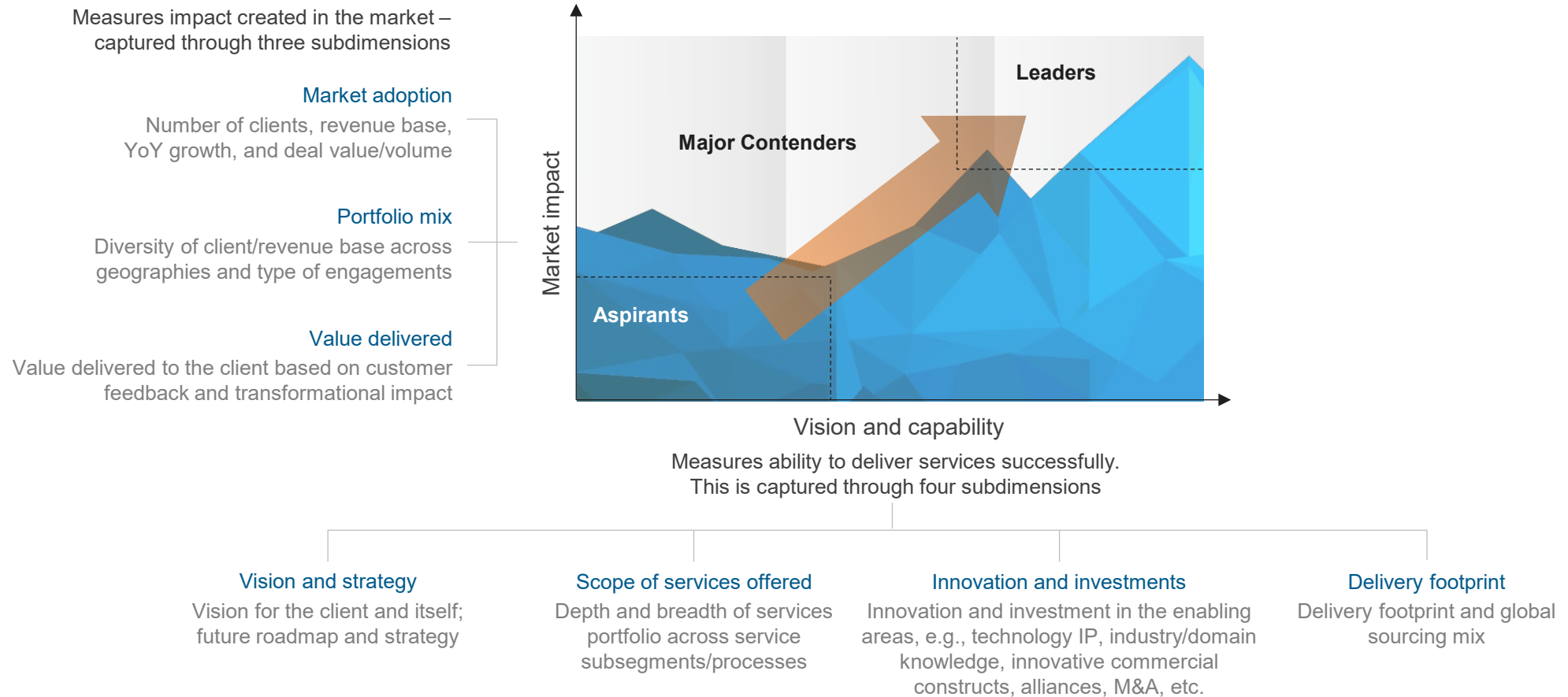
FAQs

# Everest Group PEAK Matrix® is a proprietary framework for assessment of market impact and vision and capability

Everest Group PEAK Matrix



# Services PEAK Matrix® evaluation dimensions



## FAQs

**Q: Does the PEAK Matrix® assessment incorporate any subjective criteria?**

**A:** Everest Group's PEAK Matrix assessment takes an unbiased and fact-based approach that leverages provider / technology vendor RFIs and Everest Group's proprietary databases containing providers' deals and operational capability information. In addition, we validate/fine-tune these results based on our market experience, buyer interaction, and provider/vendor briefings.

**Q: Is being a Major Contender or Aspirant on the PEAK Matrix, an unfavorable outcome?**

**A:** No. The PEAK Matrix highlights and positions only the best-in-class providers / technology vendors in a particular space. There are a number of providers from the broader universe that are assessed and do not make it to the PEAK Matrix at all. Therefore, being represented on the PEAK Matrix is itself a favorable recognition.

**Q: What other aspects of the PEAK Matrix assessment are relevant to buyers and providers other than the PEAK Matrix positioning?**

**A:** A PEAK Matrix positioning is only one aspect of Everest Group's overall assessment. In addition to assigning a Leader, Major Contender, or Aspirant label, Everest Group highlights the distinctive capabilities and unique attributes of all the providers assessed on the PEAK Matrix. The detailed metric-level assessment and associated commentary are helpful for buyers in selecting providers/vendors for their specific requirements. They also help providers/vendors demonstrate their strengths in specific areas.

**Q: What are the incentives for buyers and providers to participate/provide input to PEAK Matrix research?**

**A:** Enterprise participants receive summary of key findings from the PEAK Matrix assessment

For providers

- The RFI process is a vital way to help us keep current on capabilities; it forms the basis for our database – without participation, it is difficult to effectively match capabilities to buyer inquiries
- In addition, it helps the provider/vendor organization gain brand visibility through being included in our research reports

**Q: What is the process for a provider / technology vendor to leverage its PEAK Matrix positioning?**

**A:** Providers/vendors can use their PEAK Matrix positioning or Star Performer rating in multiple ways including:

- Issue a press release declaring positioning; see our citation policies
- Purchase a customized PEAK Matrix profile for circulation with clients, prospects, etc. The package includes the profile as well as quotes from Everest Group analysts, which can be used in PR
- Use PEAK Matrix badges for branding across communications (e-mail signatures, marketing brochures, credential packs, client presentations, etc.)

The provider must obtain the requisite licensing and distribution rights for the above activities through an agreement with Everest Group; please contact your CD or contact us

**Q: Does the PEAK Matrix evaluation criteria change over a period of time?**

**A:** PEAK Matrix assessments are designed to serve enterprises' current and future needs. Given the dynamic nature of the global services market and rampant disruption, the assessment criteria are realigned as and when needed to reflect the current market reality and to serve enterprises' future expectations.

# Stay connected

Dallas (Headquarters)

info@everestgrp.com

+1-214-451-3000

Bangalore

india@everestgrp.com

+91-80-61463500

Delhi

india@everestgrp.com

+91-124-496-1000

London

unitedkingdom@everestgrp.com

+44-207-129-1318

Toronto

canada@everestgrp.com

+1-214-451-3000

Website

everestgrp.com

Blog

everestgrp.com/blog

Follow us on



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).

## Notice and disclaimers

**Important information. Please read this notice carefully and in its entirety. By accessing Everest Group materials, products or services, you agree to Everest Group's Terms of Use.**

Everest Group's Terms of Use, available at [www.everestgrp.com/terms-of-use](http://www.everestgrp.com/terms-of-use), is hereby incorporated by reference as if fully reproduced herein. Parts of the Terms of Use are shown below for convenience only. Please refer to the link above for the full and official version of the Terms of Use.

Everest Group is not registered as an investment adviser or research analyst with the U.S. Securities and Exchange Commission, the Financial Industry Regulation Authority (FINRA), or any state or foreign (non-U.S.) securities regulatory authority. For the avoidance of doubt, Everest Group is not providing any advice concerning securities as defined by the law or any regulatory entity or an analysis of equity securities as defined by the law or any regulatory entity. All properties, assets, materials, products and/or services (including in relation to gen AI) of Everest Group are provided or made available for access on the basis such is for informational purposes only and provided "AS IS" without any warranty of any kind, whether express, implied, or otherwise, including warranties of completeness, accuracy, reliability, noninfringement, adequacy, merchantability or fitness for a particular purpose. All implied warranties are disclaimed to the extent permitted by law. You understand and expressly agree that you assume the entire risk as to your use and any reliance upon such.

Everest Group is not a legal, tax, financial, or investment adviser, and nothing provided by Everest Group is legal, tax, financial, or investment advice. Nothing Everest Group provides is an offer to sell or a solicitation of an offer to purchase any securities or instruments from any entity. Nothing from Everest Group may be used or relied upon in evaluating the merits of any investment. Do not base any investment decisions, in whole or part, on anything provided by Everest Group.

Everest Group materials, products and/or services represent research opinions or viewpoints, not representations or statements of fact. Accessing, using, or receiving a grant of access to Everest Group materials, products and/or services does not constitute any recommendation by Everest Group to (1) take any action or refrain from taking any action or (2) enter into a particular transaction. Nothing from Everest Group will be relied upon or interpreted as a promise or representation as to past, present, or future performance of a business or a market. The information contained in any Everest Group material, product and/or service is as of the date prepared and Everest Group has no duty or obligation to update or revise the information or documentation.

Everest Group collects data and information from sources it, in its sole discretion, considers reliable. Everest Group may have obtained data or information that appears in its materials, products and/or services from the parties mentioned therein, public sources, or third-party sources, including data and information related to financials, estimates, and/or forecasts. Everest Group is not a certified public accounting firm or an accredited auditor and has not audited financials. Everest Group assumes no responsibility for independently verifying such information.

Companies mentioned in Everest Group materials, products and/or services may be customers of Everest Group or have interacted with Everest Group in some other way, including, without limitation, participating in Everest Group research activities.