



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

Focus on HCLTech

July 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 Response \(MDR\) 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 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

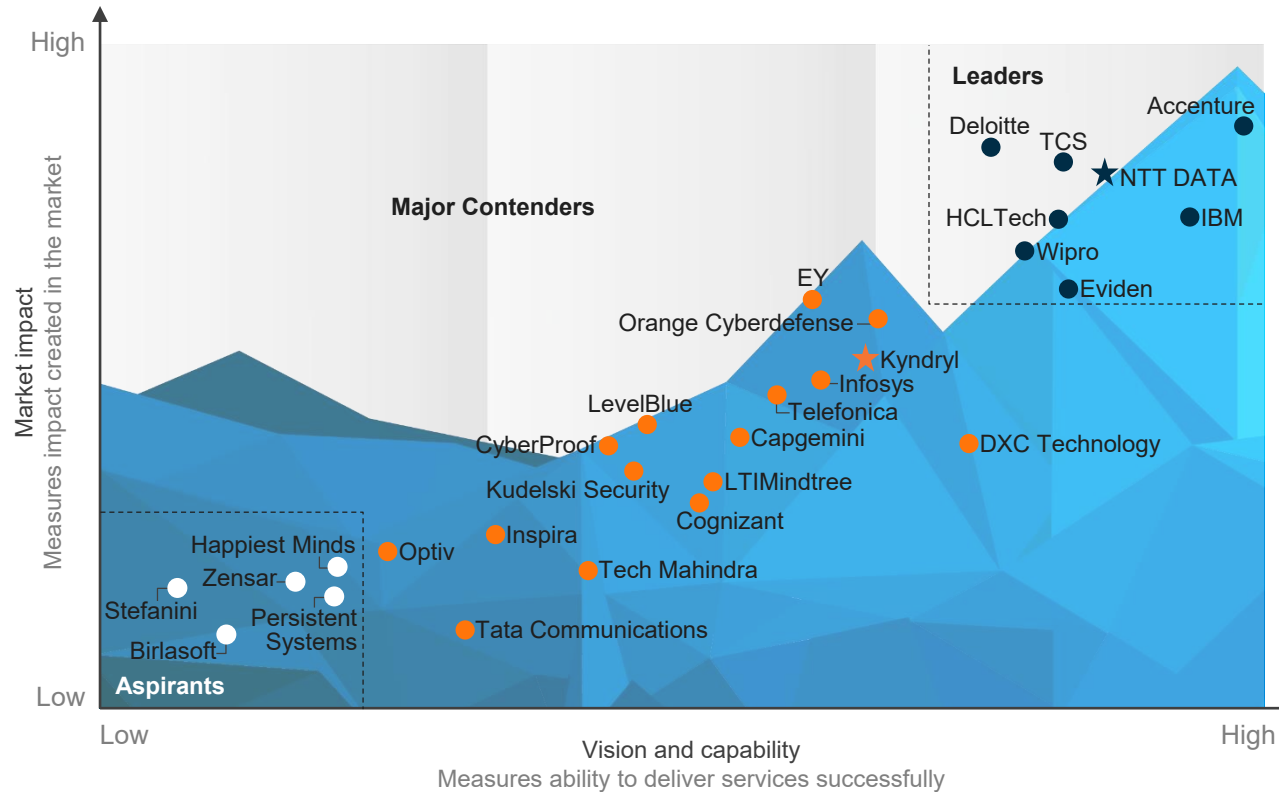
- Aspirants in the MDR market operate in niche areas and focus on addressing specific client needs, typically in small and mid-market segments
- These providers are in the early stages of developing their MDR capabilities and lack the scale to cater to large or global clients effectively
- Despite their 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 | HCLTech 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.

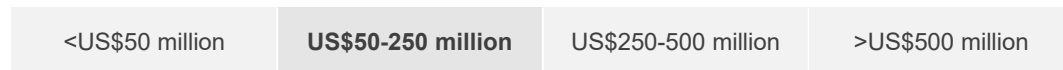
# HCLTech profile (page 1 of 6)

## Overview

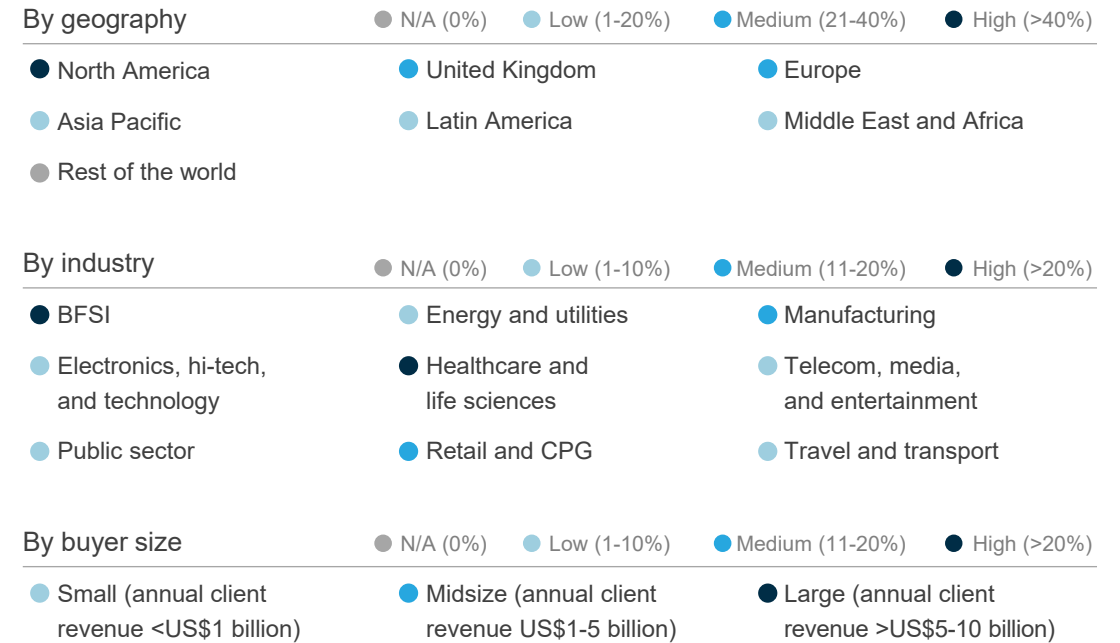
### Company mission/vision statement

HCLTech's vision for universal MDR services is to provide a one-stop solution for managed threat detection services for clients across all industry verticals and regions. It aims to help enterprises in improving their security posture and threat detection skills, therefore establishing digital trust and a secure foundation for modern enterprises. Its UMDR services help redefine security with the ultimate objective of enabling enterprise-wide visibility along with constant AI/ML led threat detection and automation-based comprehensive response support. UMDR services detect even the most elusive cyber adversaries and stay one step ahead with real-time threat intelligence and automated response capabilities. Its comprehensive suite of features, advanced automation tools, proprietary IP, and a network of technology partners including cutting-edge products, platforms, and cloud solutions together create a robust and holistic security framework for organizations.

### Overall MDR services revenue (CY 2023)



### MDR services revenue mix (CY 2023)



# HCLTech profile (page 2 of 6)

## Case studies

### CASE STUDY 1

Improved security operations and compliance for hybrid cloud workloads

**Client:** A leading energy and chemical company

#### Business challenge

The client faced challenges with complex security operations and outdated security technologies, which resulted in increased risks and poor detection capabilities. It had workloads located in hybrid cloud environments, which led to limited security visibility. It also lacked expertise in managing compliance with various regional and data protection regulations, making it difficult to navigate the complexities of regulatory requirements effectively.

#### Solution and impact

- Secured and enhanced visibility of cloud workloads through ongoing cybersecurity monitoring and management
- Minimized risks of vulnerabilities by quickly detecting and mitigating threats using security assurance services
- Automated integration of threat intelligence feeds to enable proactive threat hunting
- Assisted in achieving regulatory and compliance requirements
- Provided managed services, including cybersecurity monitoring, incident res

#### Key benefits

- Enhanced visibility of cloud workloads through continuous cybersecurity monitoring and management
- Reduced vulnerability risks by enabling rapid detection and mitigation with security assurance services
- Delivered comprehensive managed services, including cybersecurity monitoring, incident response, endpoint security, device management, and security assurance

### CASE STUDY 2

Accelerated incident response and enhanced MDR efficiency

**Client:** A leading APAC apparel manufacturer

#### Business challenge

The client faced significant delays in security operations due to manual threat investigation and response processes. Alert triage and data enrichment cycles were time-consuming, leading to slower detection and response times. High manual effort was required for incident response and escalation, further straining security operations. Additionally, the absence of automation in playbook execution and security event correlation made it difficult to efficiently manage threats, increasing the risk of security incidents going undetected or unresolved.

#### Solution and impact

- Deployed an AI-driven Unified MDR (UMDR) platform to automate alert grouping, data enrichment, and triage
- Integrated low-code security automation for faster incident response and playbook execution
- Implemented behavioral analytics to enhance detection accuracy and reduce false positives

#### Key benefits

- Incident response time reduced from 177-180 minutes per case to just three to five minutes (semi-automated)
- Automated alert grouping of 95%+, minimizing analyst workload
- Annual effort savings of 2,000+ hours through AI-driven automation
- Improvement in threat hunting efficiency by 25%, strengthening proactive security measures

# HCLTech profile (page 3 of 6)

## Solutions

[REPRESENTATIVE LIST]

### Proprietary MDR services solutions

Solution	Details
CSFC – Cyber Security Fusion Centers	It offers managed security services through next-generation CSFC powered by an advanced threat detection and response fusion platform. These CSFCs provide a unified approach to cybersecurity, ensuring that threats and risks across the enterprise IT stack are visible, detected, and responded to promptly and comprehensively through closed-loop collaboration between interdisciplinary security teams and IT domain teams.
HCLTech Fusion Platform	It allows clients to maximize their investments in existing SIEM solutions, as many can now be integrated with this platform. Additionally, the platform incorporates SOAR technology, enabling a centralized workbench for analysts to conduct proactive threat hunts, automate enrichment, and expedite responses using pre-defined custom playbooks. It features a customer dashboard that offers a snapshot of the organization's current security posture, detailing service levels and highlighting KPIs, MTTD, MTTN, and alert levels by priority.
Security Intelligence and Analytics (SecIntAI)	It is a next-generation framework for dynamic security operations known as SecIntAI. Built on this framework, CSFC provides proactive threat mitigation capabilities. By leveraging advanced big data analytics and artificial intelligence, it integrates global threat intelligence and contextual information to enhance defense against sophisticated cyber threats. It ensures a dynamic and adaptive security posture that evolves with the changing threat landscape.
Cybervigil.AI dashboard	It includes a customer interface portal designed to provide a seamless and user-friendly experience for clients. This portal serves as a single pane of glass view of the entire environment, offering a centralized platform where customers can access information and seek support, ultimately increasing satisfaction. The portal enables the collection of valuable insights through regular customer interactions and feedback.
Threat intel summarization	It delivers a summary of all critical threat intelligence feeds into IoCs and provides actionable insights by utilizing deep learning algorithms. This solution includes mapping the appropriate playbooks and automating execution to effectively remediate threats.
Security research unit	It includes a team of expert and seasoned cybersecurity professionals focused on enhancing detection and response efficiencies throughout the engagement. Its key offerings encompass collaborative threat intelligence, skilled threat hunters, threat detection and platform engineering, and critical incident handlers.
SOC reference architecture	It serves as a reference point for best practices developed and refined through experience with numerous G2000 enterprises. This solution accelerates the implementation phase by providing a best practice architecture that includes tools, processes, and skill sets necessary for effective performance.
Threat simulations	It involves proactive attacker behavior and attack path simulation to test detection efficacy, providing valuable feedback to the detection engineering team.

# HCLTech profile (page 4 of 6)

## Partnerships

[REPRESENTATIVE LIST]

### Partnerships

Partner	Type of partnership	Details
SIEM/Security analytics: Palo Alto Networks, Microsoft, CrowdStrike, Devo, and Chronicle	Technology partnership	Partnered to enhance the Fusion platform's security analytics capabilities by utilizing big data analytics and advanced correlation from next-generation security analytic tools, applying machine learning and AI algorithms to identify trends, patterns, and anomalies.
EDR: CrowdStrike, SentinelOne, and Microsoft	Technology partnership	Leveraged these partnerships to use an EDR solution and integrate it with the UMDR platform for comprehensive visibility across all endpoints, offering advanced threat detection, investigation, and response capabilities, including incident data search, alert triage, suspicious activity validation, threat hunting, and malicious activity detection and containment.
Orchestration and automation: Chronicle	Technology partnership	Partnered with various SOAR vendors, such as Google Chronicle, to enhance orchestration and automation engine capabilities, streamlining workflows and incident response processes.
Service management: ServiceNow and Tableau	Technology partnership	Partnered with ITSM and visualization firms, including ServiceNow and Tableau, to provide a comprehensive view of security alerts for customers.
Exposure management: SafeBreach, Qualys, XM Cyber, and Security Scorecard	Technology partnership	Partnered to enhance exposure management capabilities to address security risks associated with exposed digital assets, including endpoints, applications, and other cloud resources that could be exploited to breach an organization's systems, ultimately improving the overall security posture within customers' environments.
Threat intelligence: Cybersixgill, Recorded Future, and Anomali	Technology partnership	Subscribed to over 40 threat intelligence sources (both open source and paid feeds) that integrated with the Threat Intelligence platform to generate insights delivering early warnings and actionable security intelligence, enabling quick protection against threats and vulnerabilities before they impacted enterprises.
Identity analytics: Microsoft, Sailpoint, and Cyberark	Technology partnership	Partnered to enhance ITDR capabilities by monitoring identity-based risks, streamlining user access, enforcing zero trust identity access, implementing risk scoring and remediation prioritization, and conducting real-time monitoring of runtime behaviors for identity-centric IoCs, attack path management, and impact analysis.
Breach response and proactive assessments: Palo Alto Networks and Mandiant	Technology partnership	Partnered with Palo Alto and Mandiant to enhance the proactive vulnerability identification and threat management framework, providing real-time visibility to customers regarding existing threats and vulnerabilities in their environments for timely risk identification, vulnerability and patch prioritization, alternative remediation inputs, and closure of vulnerabilities before any breaches or exploitations occurred.

# HCLTech profile (page 5 of 6)

## Investments and recent activities

[REPRESENTATIVE LIST]

### Investments and recent activities

Themes	Details
Trainings/Certifications	<ul style="list-style-type: none"> <li>• It achieved Microsoft-verified MXDR solution status. By attaining this status, it demonstrated robust MXDR services, including an SOC with 24/7/365 proactive hunting, monitoring, and response capabilities, all built on tight integrations with the Microsoft security platform. This solution combined expert-trained technology with human-led services and received verification from Microsoft engineers</li> <li>• It tied up with Shiv Nadar University to introduce cybersecurity as a subject in the engineering program, facilitating the recruitment of engineers into cybersecurity teams. It also partnered with IIT Kanpur to strengthen capabilities in cybersecurity by collaborating with C3iHub, a specialized cybersecurity research center</li> <li>• It developed a specialized talent development program in collaboration with strategic partners. This initiative included special handholding sessions to assess resource backgrounds and define clear learning paths aligned with individual aspirations. It also published a monthly training calendar, offering a variety of certifications from partners and training platforms, covering topics from cloud technologies to basic conceptual understanding</li> </ul>
Investment	<ul style="list-style-type: none"> <li>• Invested in the Digital risk prevention platform, CyberSixGill, as part of a collaborative threat intelligence solution to assist customers by providing visibility into the deep and dark web; this initiative helped existing and prospective customers understand their security posture and align their security investments accordingly</li> <li>• It invested in the Security Scorecard platform as a security rating and benchmarking solution to help existing and prospective customers in understanding their security posture. This initiative aimed to help align its security investments accordingly</li> <li>• Invested in the start-up ecosystem for continuous detection of internal and external threats and vulnerabilities by conducting SaaS-based simulations and providing real-time reporting</li> <li>• It invested in Breach and Attack Simulation (BAS) platforms such as Cymulate, Safe Breach, and Pentera for continuous detection of internal and external threats and vulnerabilities. This was achieved by conducting SaaS-based simulations and providing real-time reporting</li> <li>• It invested in a strategic partnership with Devo and LogPoint to utilize big data analytics and advanced correlation of next-generation security analytic tools. Machine learning and AI algorithms were applied to identify trends, patterns, and anomalies, enhancing the capabilities of the fusion platform</li> <li>• Invested in a partnership with CardinalOps to further strengthen UMDR services by incorporating proactive threat detection, threat hunting, and continuous detection logic updates onto the Fusion platform</li> </ul>










# HCLTech profile (page 6 of 6)

Everest Group assessment – Leader

Measure of capability:  Low  High

## 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 looking for nearshore delivery options may find HCLTech’s new Cybersecurity Fusion Centers in Vietnam, Poland, and Mexico advantageous
- Enterprises seeking extensive automation will benefit from HCLTech's library of 600+ ready-to-deploy playbooks, enabling rapid response to security incidents across multiple technologies
- Enterprises seeking operational efficiency will benefit from HCLTech’s MDR services, with high SOC automation in data collection and triaging for scalable, streamlined delivery
- Enterprises looking for flexibility will find HCLTech’s customizable engagement models, including outcome-based pricing options, beneficial for optimizing costs while aligning with specific security needs
- Enterprises requiring multi-technology integration capabilities can leverage HCLTech's 150+ out-of-box integrations, allowing seamless connection across diverse security tools and platforms

### Limitations

- Enterprises seeking gen AI-driven capabilities may find HCLTech’s gen AI integration limited, as it is still in the pilot phase, delaying advanced detection benefits
- Enterprises seeking strong LATAM and MEA coverage may find HCLTech's capabilities limited, with only a recent Mexico center establishment and minimal presence in the region
- Enterprises looking for dedicated public sector expertise might face challenges, as HCLTech's MDR services show limited delivery proof points in catering to enterprises from this vertical
- Small scale enterprises may find HCLTech's emphasis on large-scale clients to be restrictive
- Clients have raised concerns about project management, noting communication gap and misaligned resource allocation

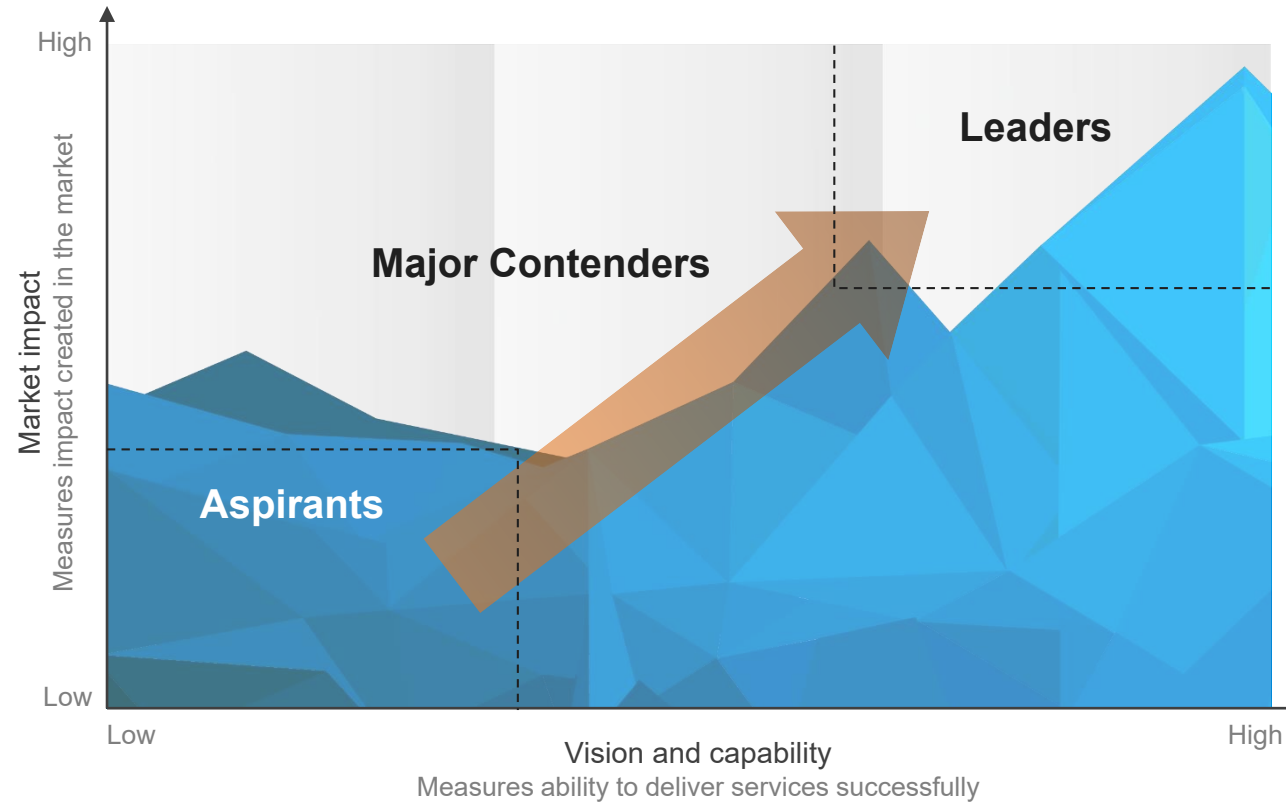
# Appendix

PEAK Matrix® framework

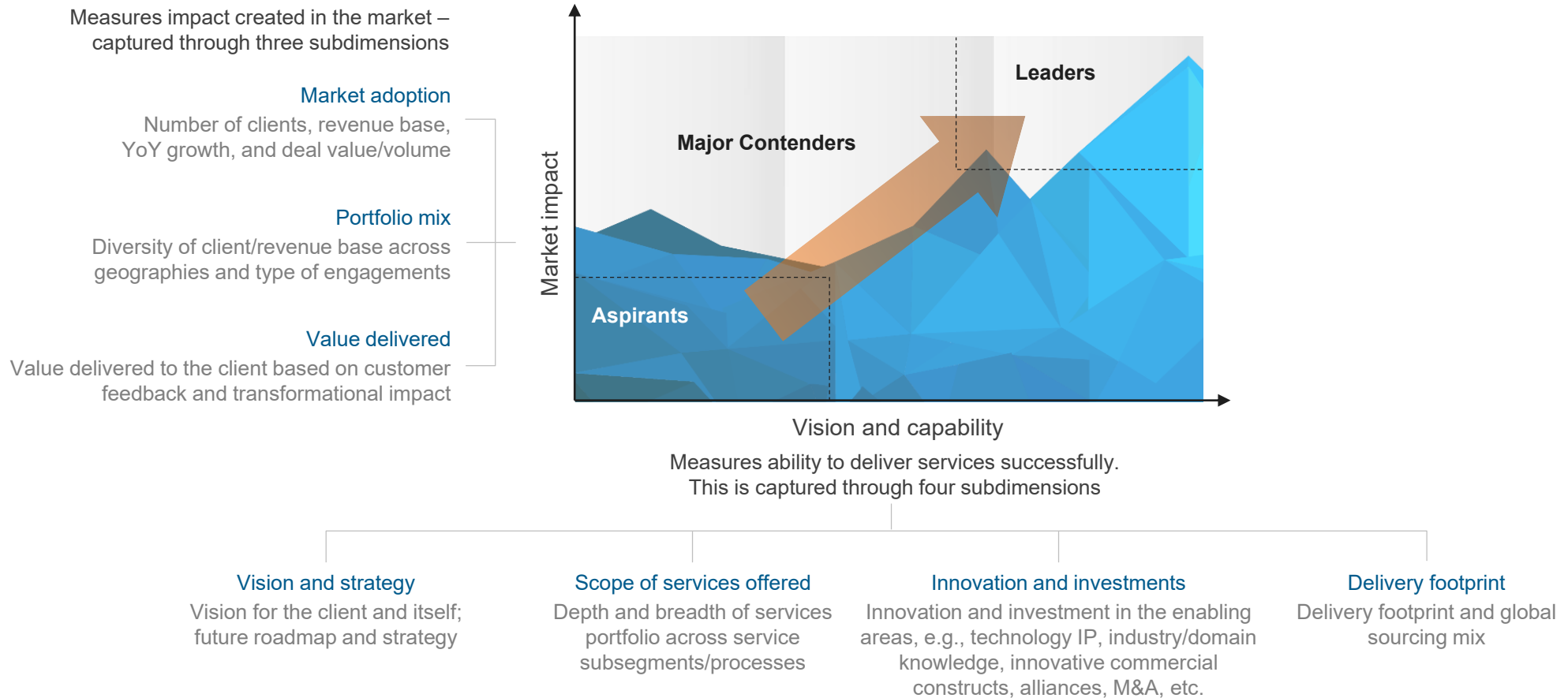
FAQs

# 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 enterprise 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.