Everest Group®

Everest Group PEAK Matrix® for Managed Detection and Response (MDR) Service Provider 2023

Focus on HCLTech

February 2023

Everest Group PEAK MATRIX®

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

MDR services PEAK Matrix® characteristics

Leaders:

Accenture, Atos, HCLTech, IBM, Orange Cyberdefense, TCS, and Wipro

- Leaders have gained significant mindshare among enterprise clients through their depth and breadth of MDR offerings. They have a strong focus on delivering comprehensive MDR services cutting across threat hunting, threat intelligence, and incident response
- Leaders have made dedicated investments in AI-/ML-based threat-hunting capabilities and have also patented ML models. Additionally, they have focused on bringing localized yet expert MDR services through industry-focused SOCs, innovation garages, and fusion centers in geographies where data residency can be a concern
- These players have showcased robust proof points around telemetry coverage from endpoints, network, IoT, OT, cloud, and SaaS. They have also developed verticalized playbooks for quicker incident response measures
- Leaders have credible add-on offerings such as attack surface management, cyber insurance quantification, dark deep web monitoring, brand protection, and ransomware readiness on top of their regular MDR services

Major Contenders:

Capgemini, Cognizant, CyberProof, Deloitte, DXC Technology, FIS Global, Happiest Minds, Infosys, Kyndryl, LTI, Microland, NTT DATA, Tech Mahindra, T-Systems, and Zensar

- These players have demonstrated high market impact in terms of YoY growth and value delivered to clients for MDR services
- While these players are increasingly investing in building MDR competencies and expertise, their capabilities in offering comprehensive telemetry coverage and verticalized playbooks still lags peers

Aspirants:

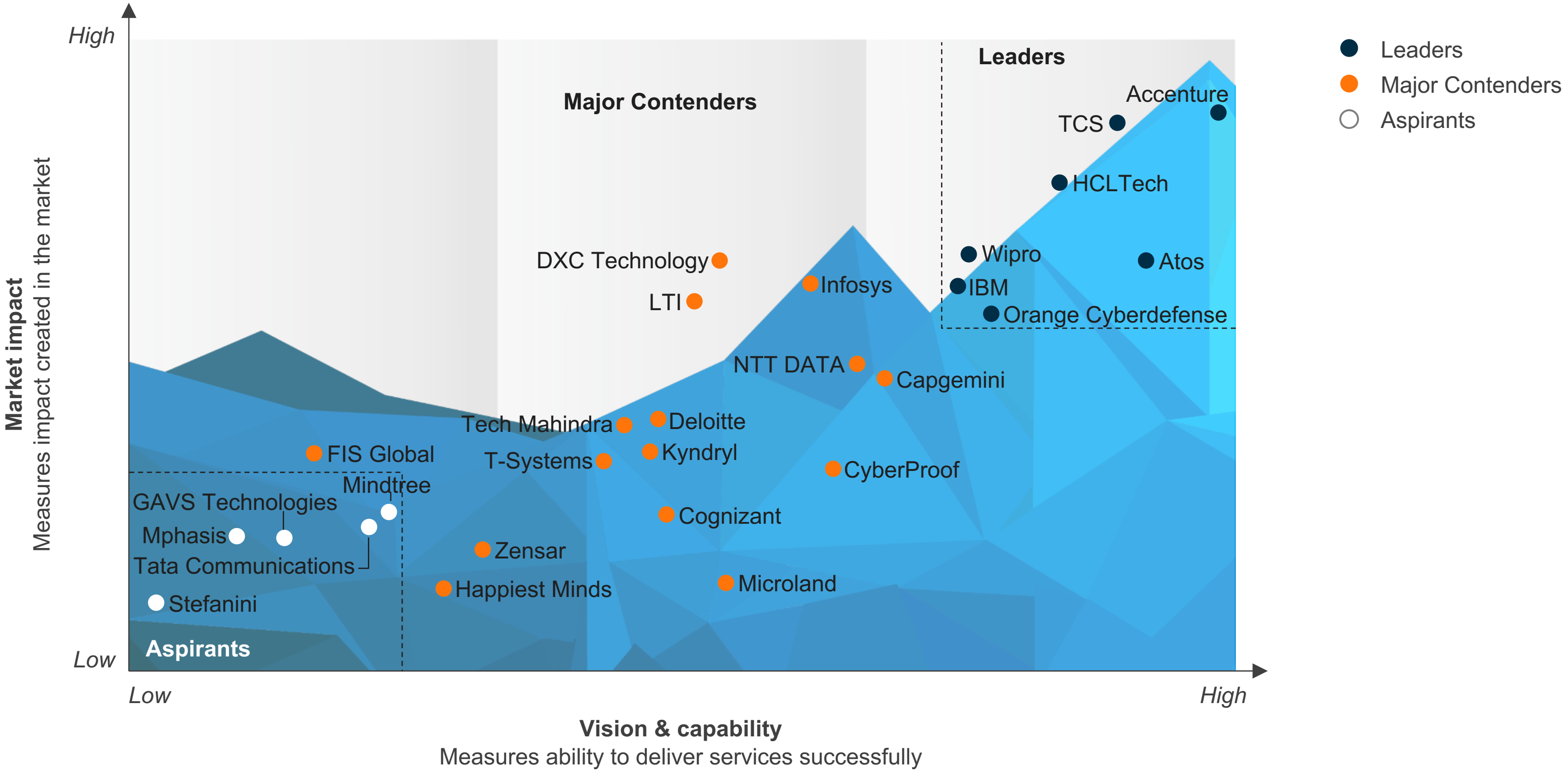
GAVS Technologies, Mindtree, Mphasis, Stefanini, and Tata Communication

- Aspirants are in the early stages of MDR services and offer limited customization flexibility to clients while choosing the technology stack for delivering MDR services
- These players rely on technology provider tools to provide MDR services instead of investing in building their own platform. Also, Aspirants tend to focus on specific verticals rather than serving clients across verticals
- Aspirants have limited add-on services as part of their MDR services portfolio and have a comparatively smaller talent pool of resources, which limits their ability to provide large-scale MDR engagements

Everest Group PEAK Matrix®

Managed Detection and Response (MDR) Services PEAK Matrix® Assessment 2022 | HCLTech positioned as Leader

Everest Group Managed Detection and Response (MDR) Services PEAK Matrix® Assessment 2022[1,2]



[1] Assessments for Capgemini, Deloitte, IBM, Kyndryl, Mphasis, and T-Systems are based on Everest Group's proprietary Transaction Intelligence (TI) database, service provider public disclosures, and Everest Group's interactions with enterprise buyers

[2] Analysis for LTI and Mindtree is based on capabilities before their merger

Source: Everest Group (2022)

HCLTech | MDR services profile (page 1 of 6)

Overview

NOT EXHAUSTIVE

Company mission/vision statement

HCLTech's vision for MDR services is to assist enterprises in eliminating cyber risks and keeping up with evolving threat dynamics while continually ensuring and safeguarding clients on their digital transformation path. The services are delivered through the FusionMDR service delivery platform with the ultimate goal to enable enterprise-wide visibility as well as continuous AI-/ML-led threat detection and automation-based complete response assistance.

MDR services revenue (2021)

<US$50 million	US$50-100 million	[✓ US$100-200 million]	>US$200 million

░ Low (<10%) ▒ Medium (10-20%) █ High (>20%)

Adoption by industry

Energy and utilities	░	Manufacturing	▒	BFSI	█
Healthcare and life sciences	█	Electronics, hi-tech, and technology	░	Retail, distribution, and CPG	░
Telecom, media, and entertainment	░	Public sector	░	Travel and transport	░
Others	░				

Adoption by buyer group

Small (annual revenue < US$1 billion)	░	Medium (annual revenue = US$1-5 billion)	▒	Large (annual revenue > US$5 billion)	█

Adoption by geography

░ Low (<15%) ▒ Medium (15-40%) █ High (>40%)

North America	█	Europe	▒	United Kingdom	▒
Asia Pacific	░	Latin America	░	Middle East & Africa	░
Rest of the World	░				

HCLTech | MDR services profile (page 2 of 6)

Case studies

Case study 1 | Enhance the overall security monitoring

Client: a Fortune 500 American manufacturer of industrial tools and household hardware and a provider of security products

Business challenge

The client has multiple technologies tools with limited centralized visibility into the overall security posture and across geographies

Solution

Through HCLTech's Fusion Platform, HCLTech enabled the client to deploy, manage, and deliver Fusion MDR services for enhanced enterprise-wide security visibility, proactive threat detection & threat hunting, and superior automated response actions to cater to immediate threats.

Key benefits

HCLTech integrates multiple security technologies to enrich the data flow on the monitoring platform and provided the following services:

- Delivered continuous security platform monitoring and management resulting in contextual awareness and enterprise-wide visibility
- Enhanced the overall security posture for the customer by developing custom detection & response use cases and delivering cost-effective prevention, detection, and response services for multiple security solutions
- Enabled single dashboard visibility of all the security artifacts
- Enabled cost-effective services with predictability and lower Total Cost of Ownership (TCO) superior outcome-based Transmission and Distribution Business of the Licensee and the Retail Business (TD&R)

Case study 2 | Visibility to security environment using standard MDR services

Client: a global transportation, logistics, and storage company

Business challenge

The client had zero to limited visibility into the security environment due to the presence of fragmented security technologies and the presence of multiple third-party service providers.

Solution

HCLTech works with the client through its Fusion platform to deliver MDR services to bring industry standards to the client's environment at all levels including talents, processes, and technology.

Key benefits

To enhance the overall security posture, HCLTech offered a modular and scalable approach to limit the expense of cybersecurity and delivered end-to-end MDR services and achieved the following:

- Enabled faster time to detect & respond to immediate threats with coverage across endpoints, networks, cloud, infrastructure, and apps
- Optimized the entire environment through add-on services such as proactive assessment and enhancement
- Realized the benefit of the existing security investment by leveraging existing security tool sets to the full degree
- Acted as the single touchpoint with capabilities across the security spectrum leading to vendor consolidation at the customer end

HCLTech | MDR services profile (page 3 of 6)

Solutions

Proprietary solutions (representative list)

Solution name	Details
Cybersecurity Fusion Centers (CSFC)	HCLTech's cybersecurity fusion centers are powered by its advanced threat detection & response Fusion Platform. This has helped its customers to eliminate the siloed SIEM or endpoint-focused approach and adopt a more holistic, dynamic threat detection and response service covering the full spectrum from cloud to on-premise & industrial OT.
HCLTech Fusion Platform	HCLTech has invested in building a threat detection and automated response-based platform called HCLTech FUSION Platform that offers extended threat detection & response and enables HCLTech to deliver vastly improved and enhanced services to its monitoring/MDR customers
HCLTech FusionMDR	HCLTech Fusion Managed Detection and Response (MDR) is a full-suite threat detection and response stack delivered to the customer in a service and turnkey model built on a next-generation fusion platform and remote services delivered out of its CSFCs, located strategically across the globe.
Security analytics	Security analytics is delivered through the Fusion Platform modules and includes an advanced User and Entity Behavior Analytics (UEBA) solution. This is capable of quick detection and taking pre-authorized response actions to any insider threats and threats focused on internal end-users.
Security Intelligence and Analytics (SecIntAI)	The HCLTech SecIntAI framework is a proactive threat mitigation product that uses big data analytics and AI to prevent sophisticated attacks while detecting and responding to threats using global threat intelligence and contextual information. The following modules comprise the SecIntAI framework: ● **Data collection and correlation:** timely log collection and correlation from all sources ● **Vulnerability and risk management:** assessment of vulnerabilities, threat modeling, risk assessment, and prioritization ● **Collaborative threat intelligence**: integration of global threat intelligence and rule updates ● **Incident response:** AI-enhanced and automated incident response and forensic help
Digital Threat Intel (DTI)	HCLTech also offers digital threat intelligence as part of its MDR portfolio. HCLTech DTI service can discover and validate digital risks to a specific organization by monitoring the widest range of intel data sources within the visible, deep, and dark web to protect the company's business and reputation.
HCLTech Fusion EDR	HCLTech has enhanced its MEDR services with its integration with its Fusion Platform, which helps in preventing but proactively detecting threats focused on endpoints.
Vulnerability Management for Enterprise Security (VERITY)	VERITY is a holistic vulnerability management program that takes a risk-focused approach to identify and respond to vulnerabilities within a particular environment.
Collaborative Threat Intelligence	HCLTech offers collaborative threat intelligence services that take feeds from 40+ threat intelligence sources (open source and paid feeds) and generate insights that deliver early warnings and actionable security intelligence to an enterprise, enabling them to quickly protect against threats and vulnerabilities before they impact an enterprise.
CSFC Dashboard	The HCLTech CSFC Dashboard is a web-based dashboard that provides up-to-date visibility into the customer's security posture with a comprehensive view of alerts, case analysis, and incident standpoints. It visually represents the critical security threats that customer environments face through widget-based views.

HCLTech | MDR services profile (page 4 of 6)

Partnerships

Partnerships (representative list)

Partner name	Type of partnership	Details of the partnership
Google	Service partnership	HCLTech has a strategic partnership & joint GTMs on the ground, also laid out with investments in a dedicated CoE to cater to Google's environment and its security investments. HCLTech is one of the only GSIs with the highest level of security partnership certifications.
Palo Alto	Service partnership	HCLTech has forged a Global MSSP arrangement with Palo Alto Networks Inc. (PANW) to co-create a joint solution offering, which is backed by a robust GTM strategy laid out by the leadership.
Cyberbit	Technology partnership	HCLTech has invested in this platform to co-create lab use cases and conduct problem and solution simulations in a secure cyber range environment to test a variety of use cases and bring in the attackers' context.
XM Cyber	Technology partnership	HCLTech and XM Cyber are working together for the continuous detection of internal and external threats/vulnerabilities by carrying out SaaS-based simulations and enabling real-time reporting.
IBM	Technology partnership	HCLTech has a strategic partnership with IBM to jointly take to market an advanced security analytics offering.
Microsoft	Technology partnership	● HCLTech has a strategic partnership and joint GTMs on the ground, also laid out with investments in a dedicated CoE to cater to Microsoft's environment. ● HCLTech has a strategic partnership with Microsoft to jointly take to market advanced threat detection offerings.
Proofpoint	Technology partnership	It has a technology partnership with Proofpoint to jointly take to market an advanced security analytics offering that is focused on end-user security
Armis	Technology partnership	HCLTech, to strengthen its IoT & OT security threat detection and response capabilities, has partnered with Amis to develop joint offerings around ICS security solutions. This partnership has enabled HCLTech to cater to its clients' highly verticalized use case demands.

HCLTech | MDR services profile (page 5 of 6)
Investments and recent activities

Investments and recent activities (representative list)

Themes	Details
Acquisitions	HCLTech, as the part of Mode 3 strategy, has acquired select IBM Products and is now delivering services leveraging them in the areas of MDR, application security, data security, and endpoint security
Talent & Training	● HCLTech has established cybersecurity as a topic in Shiv Nadar University's Engineering curriculum and had such engineers hired into the cybersecurity teams ● HCLTech has also collaborated with IIT Kanpur. HCLTech will partner with C3iHub, a specialist cybersecurity research center at IIT Kanpur, to strengthen its expertise in the field of cybersecurity ● HCLTech has teamed with Microsoft, AWS, Azure, and CISCO to begin on a path of certification upskilling. Such certification programs have been created by the dedicated BU teams ● HCLTech has an in-house Learning Management System (LMS) with co-produced and in-house developed material on several securities and non-securities issues, as well as learning pathways for personas ranging from freshers to senior executives
Others	● **Development:** HCLTech has been continuously focused on co-creating & co-innovating with and for its customers. It has enabled a co-innovation lab to conduct joint workshops with its enterprise customers and simulate real-world business problems and propose targeted solutions to elevate their overall security posture ● **Extended threat detection & response:** HCLTech has invested in building a threat detection and automated response-based platform called HCLTech FUSION Platform, which enables HCLTech to deliver vastly improved and enhanced services to its monitoring/MDR customers ● **Threat hunting:** HCLTech has invested in and is continuously improving its threat-hunting capabilities. To disarm the attacks proactively, CSFC analysts stay vigilant of IOCs/ IOAs and common vulnerabilities, which trigger their hunt for threat vectors in the customer's environment

HCLTech | 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
◕	◕	●	◕	◕	◑	●	◕	◕

Strengths

- Enterprises searching for a service provider that can provide comprehensive telemetry coverage can evaluate HCLTech’s FusionMDR platform, which offers coverage across endpoints, cloud, SaaS, IoT, and OT devices
- Enterprises can benefit from HCLTech's investments in building the Cyber Design Center, which enables it to co-innovate and work more closely with clients through real-time attack simulation on clients’ IoT/OT infrastructure
- Some clients have highlighted technical expertise and price competitiveness as major strengths for HCLTech
- Enterprises will find HCLTech attractive because of its investments in building a well-spread network of SOCs and Cyber Security Fusion Centers (CSFC), which allows it to deliver localized yet expert MDR services
- Enterprises with high-fidelity alerts as a critical criterion can benefit from HCLTech's SecIntAI solution for delivering AI-enabled contextualized threat intelligence

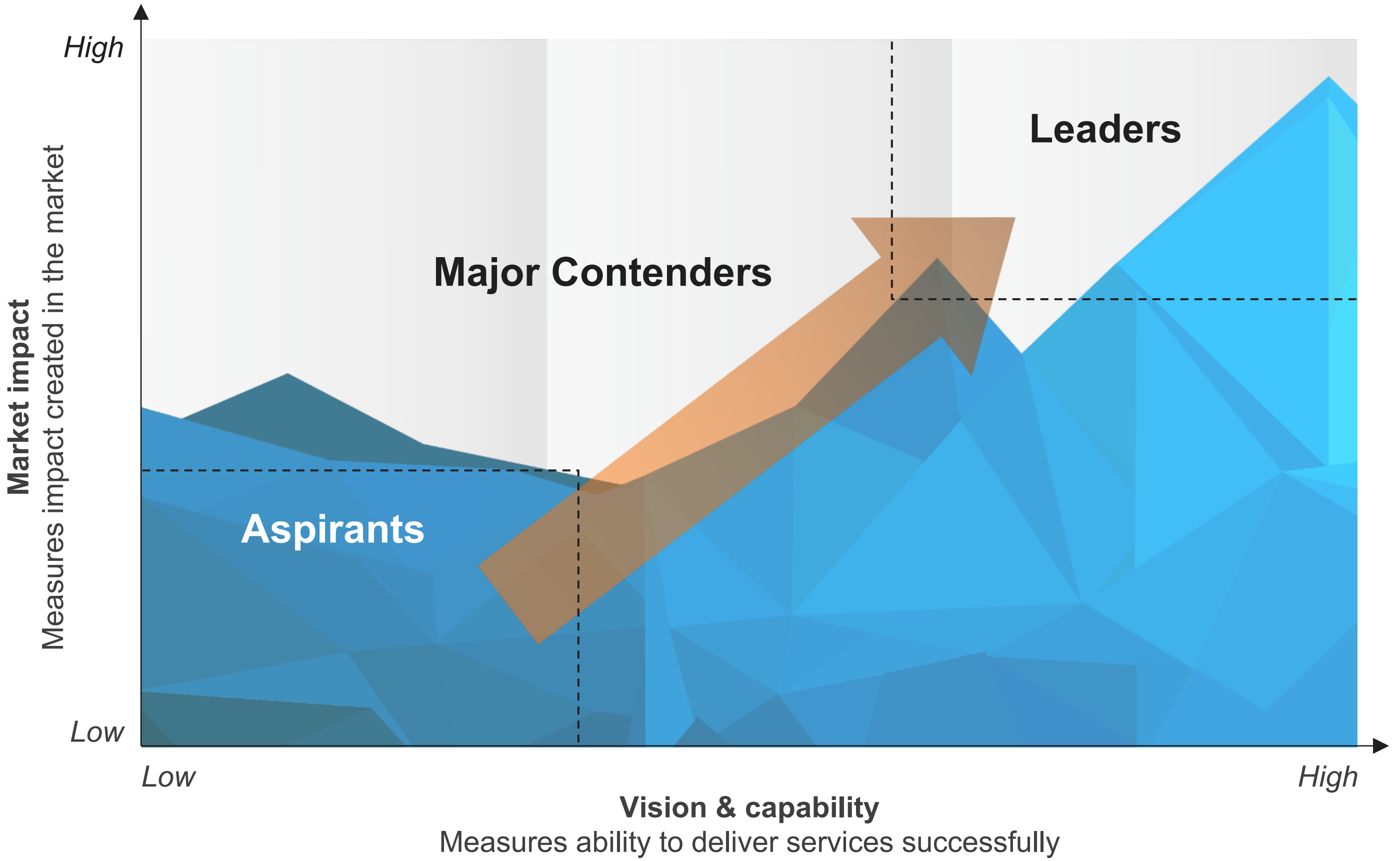
Limitations

- Enterprise searching for a service provider with a robust onshore presence should carefully assess HCLTech as the majority of its talent is offshore
- Enterprises from retail, CPG, & distribution, electronics, hi-tech, & technology, and public sector verticals should be wary that HCLTech lags peers in terms of presence within these industries
- A few clients believe that HCLTech can improve its threat-reporting capabilities
- Some clients have highlighted that the internal communication and cooperation among HCLTech's security teams are a challenge
- Some clients have highlighted the limited visibility of HCLTech's newly built IP as a challenge, and they believe that HCLTech can bring about a formal strategy to evangelize the newer solutions to the incumbent clients

Appendix

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

Everest Group PEAK Matrix


High
Low
Market impact
Measures impact created in the market
Leaders
Major Contenders
Aspirants
Low
High
Vision & capability
Measures ability to deliver services successfully

Services PEAK Matrix® evaluation dimensions

Measures impact created in the market – captured through three subdimensions

Market adoption

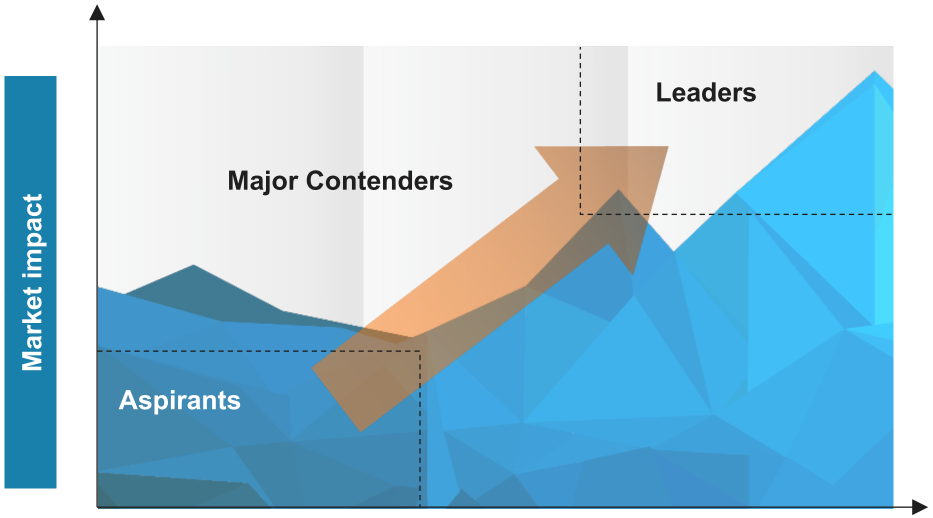
Number of clients, revenue base, YoY growth, and deal value/volume

Portfolio mix

Diversity of client/revenue base across geographies and type of engagements

Value delivered

Value delivered to the client based on customer feedback and transformational impact



Vision & capability

Measures ability to deliver services successfully. This is captured through four subdimensions

Vision and strategy

Vision for the client and itself; future roadmap and strategy

Scope of services offered

Depth and breadth of services portfolio across service subsegments/processes

Innovation and investments

Innovation and investment in the enabling areas, e.g., technology IP, industry/domain knowledge, innovative commercial constructs, alliances, M&A, etc.

Delivery footprint

Delivery footprint and global sourcing mix

FAQs

Does the PEAK Matrix® assessment incorporate any subjective criteria?
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.

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

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

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

- 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 in included in our research reports

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

- 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

Does the PEAK Matrix evaluation criteria change over a period of time?
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.

Everest Group®
With you on the journey

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**.

Stay connected

Website
everestgrp.com

Social Media
@EverestGroup
@Everest Group
@Everest Group
@Everest Group

Blog
everestgrp.com/blog

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
+1-647-557-3475

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.