Everest Group®

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

Focus on TCS

March 2025

PEAK MATRIX®

Introduction

As enterprises 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

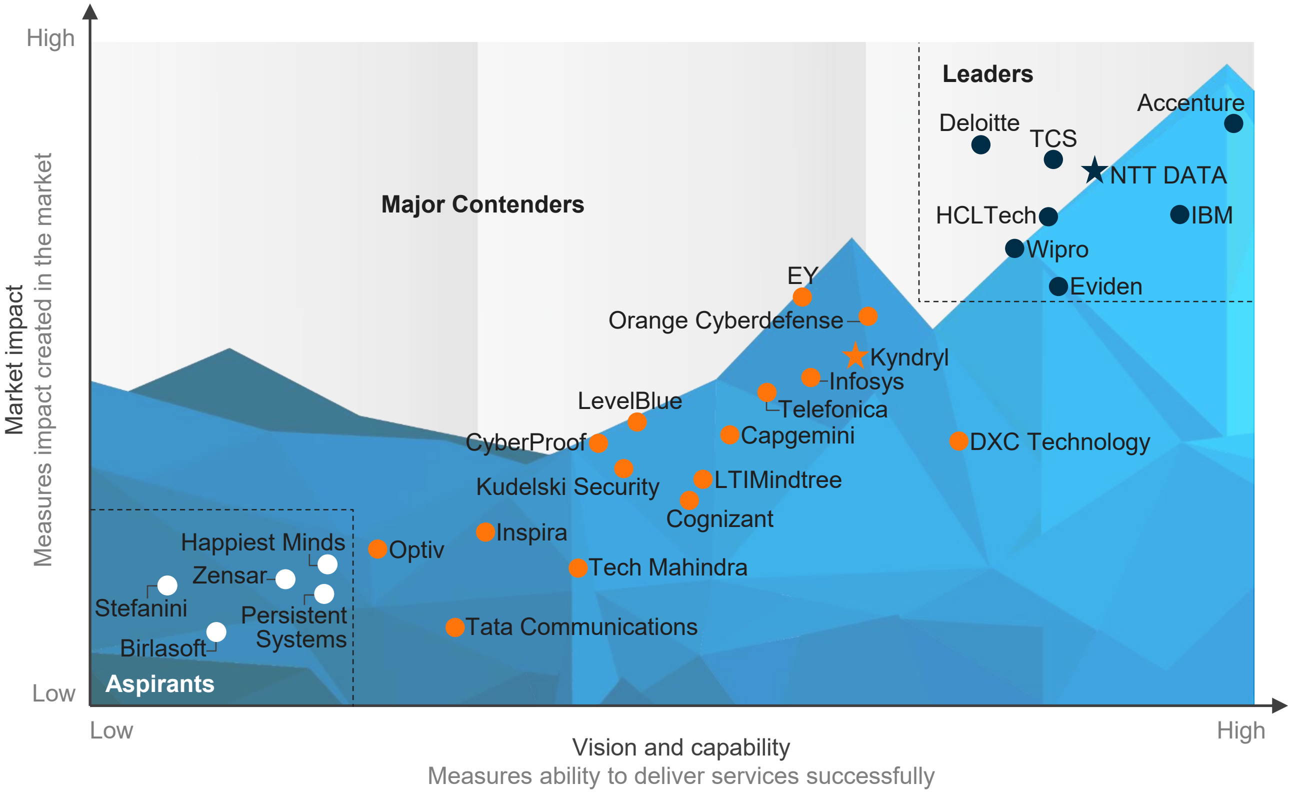
- Aspirants in the MDR market operate in niche areas and focus on addressing specific client needs, typically in small and mid-market segments
- These providers are in the early stages of developing their MDR capabilities and lack the scale to cater to large or global clients effectively
- Despite their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

Everest Group Managed Detection and Response (MDR) Services PEAK Matrix® Assessment 2025[1]

- ● Leaders
- ● Major Contenders
- ○ Aspirants
- ☆ Star Performers



[1] 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

TCS profile (page 1 of 8)

Overview

Vision

TCS aims to be a leader in the industry by improving security and detection across a growing attack surface including AI and quantum threats. The goal is to deliver results-driven, measurable services tailored with industry expertise and threat intelligence to detect and contain threats. Its vision includes using AI to enhance detection and response automation, supported by human expertise for customer experience, and to secure customer technology adoption including AI model protection. It aims to provide transparent service levels with visibility across endpoints, networks, identities, and cloud workloads through the TCS Cyber Defense Suite. It plans to enhance cyber resilience through exposure validation and attack simulations. A key part of its vision is to leverage technology partnerships and co-innovation through the TCS COIN™ network to deliver faster value to customers.

MDR services revenue (CY2023)

<US$50 million	US$50-250 million	US$250-500 million	**>US$500 million**

MDR services revenue mix (CY 2023)

By geography — ◌ N/A (0%) ○ Low (<15%) ◐ Medium (15-40%) ● High (>40%)

- ● North America
- ◐ United Kingdom
- ◐ Europe
- ○ Asia Pacific
- ○ Middle East and Africa
- ○ Rest of the World
- ○ LATAM

By industry — ◌ N/A (0%) ○ Low (<10%) ◐ Medium (10-20%) ● High (>20%)

- ● BFSI
- ◐ Energy and utilities
- ◐ Manufacturing
- ◐ Healthcare and life sciences
- ○ Electronics, hi-tech, and technology
- ○ Telecom, media, and entertainment
- ○ Public sector
- ◐ Retail and CPG
- ○ Travel and transport

By buyer size — ◌ N/A (0%) ○ Low (<10%) ◐ Medium (10-20%) ● High (>20%)

- ○ Small (annual client revenue <US$1 billion)
- ◐ Midsize (annual client revenue US$1-5 billion)
- ● Large (annual client revenue US$5-10 billion)

TCS profile (page 2 of 8)

Case studies

CASE STUDY 1

Enhanced SOC productivity and improved security operations

Client: One of the world's largest airline group

Business challenge

The client faced challenges in enhancing SOC productivity, particularly with incident response and security posture management. There were also difficulties in improving security reporting, which impacted the overall effectiveness of its security operations.

Solution and impact

- Explored multiple approaches to optimize and transform security operations, streamlining threat detection and response
- Integrated various tools through APIs with M365 Defender XDR, Entra, Intune, and other Microsoft-native solutions
- Implemented just enough access for the SOC and Defender Security Engineering team, ensuring necessary privileges to effectively utilize copilot capabilities for real-time assessment and analysis of security incidents
- Generated executive summary reports based on automated analysis from multiple integrated tools, providing insights on security investigations, publicly disclosed vulnerabilities, and threat actors along with their campaigns

Key benefits

- Optimized SOC costs by increasing operational efficiency and effectiveness
- Enhanced L1 investigations, accelerating the speed of investigative processes
- Reduced manual efforts and shortened the mean time to detect and respond to threats in real time
- Streamlined the extraction and summarization of information for security reporting and analytics

TCS profile (page 3 of 8)

Case studies

CASE STUDY 2

Provided managed security services for overall SOC operations detection and response

Client: A leading British multinational automobile manufacturer

Business challenge

The client lacked best practices and process documentation, which increased the time and effort needed to understand the existing environment and create a security roadmap. Its inadequate integration of log sources with Chronicle led to ineffective management and underutilization of the tool. Excessive false positives indicated a need for fine-tuning of detection rules in Chronicle. There were also issues with the implemented content, and no steps were taken to identify gaps or troubleshoot problems. The operation of multiple security tools in isolation, without correlation, presented a challenge for SOC analysts who had to monitor multiple consoles to determine the impact of security events.

Solution and impact

- Established a 24x7 SOC for security incident detection, response, management, and remediation
- Maintained and managed log sources, ensuring seamless integration with SIEM and SOC tools
- Provided use cases aligned with the MITRE ATT&CK® framework for enhanced threat detection and response
- Delivered vulnerability assessment services for both on-premise and cloud assets maintained in the CMDB
- Conducted monitoring and analysis through a threat intelligence platform, covering the surface web, deep web, and dark web based on the current watchlist to proactively detect and mitigate potential cyber threats

Key benefits

- Improved MITRE coverage from 30% to 68.94% by integrating multiple log sources with the SIEM
- Configured multiple use cases in Splunk and Chronicle for various security detection scenarios
- Enhanced coverage and detection, while reducing the false positive ratio for SOC monitoring from 70% to 30%
- Successfully upgraded Splunk Enterprise and its architecture
- Automated phishing response and implemented additional playbooks using the SUMO Logic SOAR solution
- Deployed Vulcan for risk-based vulnerability management
- Implemented email triage automation for auto ticket creation in the SOC mailbox
- Proposed a SOC transformation plan focused on automation, gen AI, and SOAR to reduce efforts and costs

TCS profile (page 4 of 8)

Solutions

[REPRESENTATIVE LIST]

Proprietary MDR services solutions

Solution	Details
MVP baseline detection library	It provides adequate visibility across customer environments by utilizing TCS' proprietary detection rules.
Automation playbook library	It utilizes TCS' proprietary modular automation playbooks to improve the mean time to respond to and contain incidents effectively.
I2A2 framework for IR automation	It provides a framework to systematically identify potential automation opportunities within detection rules, along with a streamlined process to enable full workflow automation.
Gen AI prompt library for analyst assistance	It provides a gen AI prompt library to support leading security technologies and platforms, assisting security analysts with their investigations.
Threat intel platform	It serves as a threat intelligence platform for aggregating, prioritizing, and timely disseminating operational intelligence across TCS' customer base.
Threat briefings	It delivers periodic threat advisories containing tactical and strategic inputs tailored to specific industries and geographical regions.
Detection and response reference architecture	It establishes an updated reference architecture for detection and response, designed to support next-generation MDR services.
TCS Cyber Defense Suite (CDS) – Cyber Intelligence	It offers cyber observability-as-a-service, providing customers with comprehensive visibility into cybersecurity posture. It offers flexibility/adaptability to incorporate the organization structure (conglomerate, M&A, and heavily regulated), nature of business, risk appetite, and security goals and helps enterprise leaders set benchmarks, identify the gaps, measure progress, and communicate to stakeholders.
TCS Cyber Defense Suite (CDS) – Cyber Vigilance module	It provides threat detection and response capabilities to customers as-an-MDR service. This module includes core service components such as SIEM, threat intel platform, and SOAR, with optional services such as threat surface management, deception, threat hunting, Incident Response (IR), and digital forensics.
Ransomware Controls Matrix (RCX)	It enhances organizational readiness against ransomware threats.

TCS profile (page 5 of 8)

Solutions

[REPRESENTATIVE LIST]

Proprietary MDR services solutions

Solution	Details
Zero Trust Operating Model (ZTOM)	It provides zero-trust holistic transformation.
Gen AI use cases for detection and response	TCS developed an AI security workbench capability to build and prototype various gen AI solutions including threat detection and response solutions. Several use cases were developed such as SOC assistant, log analyzer, guided investigation, and compliance assistant.
Gen AI security workbench and gen AI security use cases	TCS built machine learning models to detect anomalies in connected infrastructure.
AI/ML detection library	TCS invested in building a cyber insight and analytics solution as part of the cyber defense suite. This solution was designed to analyze security logs, events, and telemetry to identify anomalous behavior and abnormal patterns, enabling the detection of potential indicators of cyberattacks.

TCS profile (page 6 of 8)

Partnerships

[REPRESENTATIVE LIST]

Partnerships

Partner	Type of partnership	Details
Crowdstrike	Technology partnership	It partnered with CrowdStrike to secure endpoints and enhance detection and response capabilities, as well as to utilize threat intelligence and threat hunting services. It trained a large pool of resources on CrowdStrike's next-generation SIEM, which included automation and gen AI (Charlotte) capabilities. TCS also leveraged CrowdStrike's Engagement License Program (ELP) to support its consulting and advisory services, covering incident response, endpoint, and identity posture assessments, among others.
Microsoft	Technology partnership	Partnered with Microsoft to leverage SIEM and XDR solutions.
Google	Technology partnership	It partnered with Google to enhance TCS's MDR platform services, which were powered by Google SecOps. Additionally, the collaboration leveraged the Google ecosystem including Mandiant components for threat intelligence, control validation, and other functionalities.
Rapid7	Technology partnership	It partnered with Rapid7 to leverage threat intelligence, brand protection, and dark web monitoring. It also collaborated with Rapid7 on its detection and response platform to develop an alternative MDR platform offering that could provide a per-asset-based Resource Unit (RU) model.
Recorded Future	Technology partnership	Partnered with Recorded Future to utilize its services for threat intelligence, brand protection, and dark web monitoring.
IBM	Technology partnership	Partnered with IBM to leverage advanced AI for threat detection and response for endpoints, enhance threat detection and prioritization for real-time visibility, and implement automation and workflow management for security operations.
Palo Alto	Technology partnership	Partnered with Palo Alto to leverage its solutions for endpoint protection, extended detection and response, ransomware protection, digital forensics, orchestration and automation, threat intelligence, and attack surface management.
XM Cyber	Technology partnership	Partnered with XM Cyber to leverage continuous threat exposure management for risk exposure reduction and SOC optimization.
Hoxhunt	Technology partnership	Partnered with Hoxhunt to implement a solution for phishing awareness training and simulation campaigns across various environments.
Cymulate	Technology partnership	Partnered with Cymulate to leverage breach and attack simulation for various threat vectors including endpoint, email, and network.

TCS profile (page 7 of 8)

Investments and recent activities

[REPRESENTATIVE LIST]

Investments and recent activities

Theme	Details
Delivery centers	TCS established a global network of 13 cybersecurity delivery centers strategically chosen to provide localization, meet data sovereignty and retention requirements, and address local compliance and regulatory needs.
Investments	TCS maintained a focus on R&D, with investments ranging from 3-4% of the total revenue. It has a dedicated Research and Innovation (R&I) unit, led by the Chief Technology Officer (CTO). The R&I unit was responsible for delivering improvements to current offerings and creating a pipeline for new business solutions. It actively scanned the technology horizon, preparing TCS for emerging technologies in both the near term and long term.
Talent/Certifications	• Partnered with academic institutions to drive mutually beneficial growth by expanding the addressable market, co-creating joint security solutions, fostering talent development, promoting innovation, and advancing thought leadership • Invested in recruiting cybersecurity experts from big four firms and other key areas to interface with boards, CISOs, and key customer leadership across service lines, primarily focusing on security strategy advisory and consulting • Invested in Coimbatore Institute of Technology (CIT) for lab setup, training, and skill development to build a readily deployable pool of cyber-skilled professionals • Launched its flagship STEM education program, GoIT, benefiting students worldwide since its inception in 2009. Rooted in design thinking, the program introduced students to the innovation life cycle and rapid prototyping framework • Initiated a cybersecurity internship program in collaboration with the University of Miami, Ohio, with the curriculum strategically designed to cover key areas such as AI, incorporating both discriminative and generative models • Allocated focused budgets for certification drives, reimbursements, and partner-led certification programs for Okta, CyberArk, Thales, cloud security-themed certifications (MS Azure, AWS, and Google Cloud), CompTIA Security+, Zscaler, PING, and CISM certifications • Implemented FrescoPlay, enabling employees to access training modules seamlessly across mobile and web devices • Invested in an innovative recruitment approach through the gamified hiring contest, HackQuest, to attract cybersecurity talent
TCS COIN™	TCS invested in TCS COIN™, a global network that brought together experts from start-ups, research, academia, and corporate sectors to collaborate on innovations for Fortune 1000 customers. The network included 2,500 start-ups from the US, Israel, Canada, Europe, and India, supported by nearly 50 university partners and numerous cybersecurity firms.

TCS profile (page 8 of 8)

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 seeking global MDR coverage can benefit from TCS's extensive network of Security Operations Centers and Fusion Centers across North America, Europe, APAC, and other regions
- Enterprises seeking integrated threat management can leverage TCS's Cyber Defense Suite that provides unified visibility across endpoints, networks, identity, and cloud workloads
- Enterprises needing industry-specific MDR solutions will benefit from TCS's domain-aligned service offerings tailored for different sectors' unique risk profiles
- Enterprises seeking comprehensive OT security coverage can benefit from TCS's specialized partnerships with Claroty, Tenable, and Microsoft for industrial systems monitoring
- Enterprises seeking to enhance SOC productivity can leverage TCS's gen AI-powered assistant for accelerated incident triaging, analysis, and guided response based on integrations with Microsoft security tools

Limitations

- Enterprises seeking highly skilled MDR resources may find limitations with TCS, as clients have raised concerns about potential skill gaps within their workforce
- Clients have expressed that TCS should take a more proactive and strategic approach, offering insights and recommendations beyond the immediate scope of work
- Enterprises belonging to public sector and telecom, media, and entertainment may find limitations with TCS's MDR services due to its relatively lower focus on this vertical
- Enterprises in the small scale segment may find TCS's focus on large and medium-scale industries limiting
- Enterprises seeking cost-effective MDR services may face challenges, as some clients have cited TCS for its premium pricing

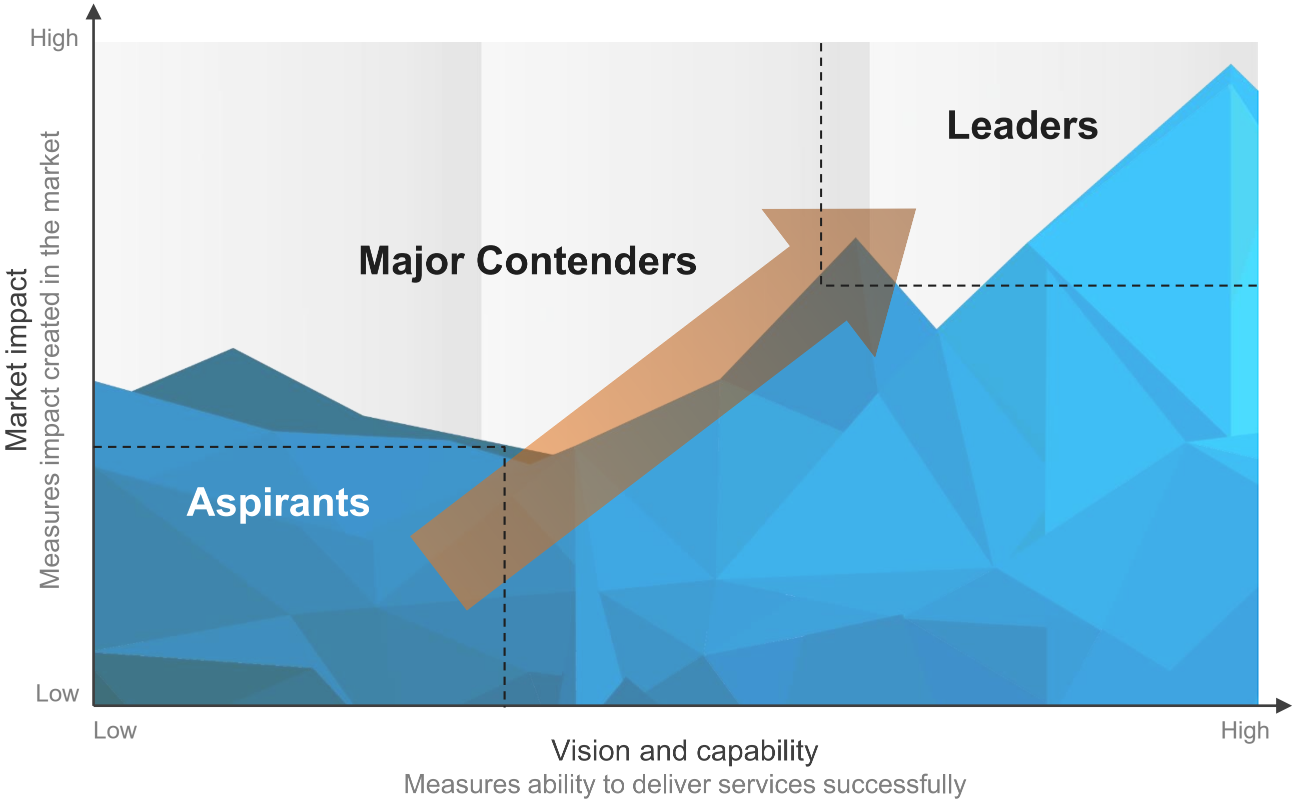
Appendix

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


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

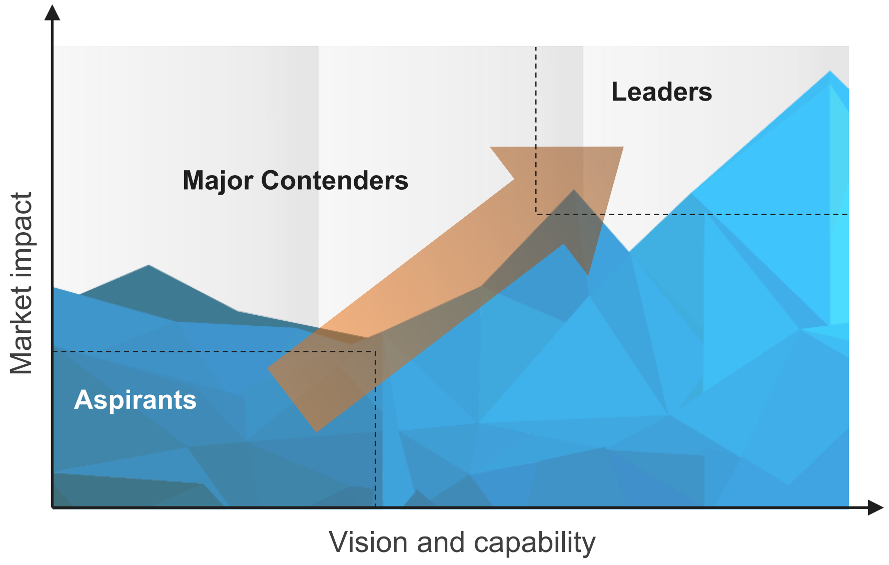
Services PEAK Matrix® evaluation dimensions

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



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

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 in 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**.

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, 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.

Everest Group®
With you on the journey