Everest Group®

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

Focus on NTT DATA

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

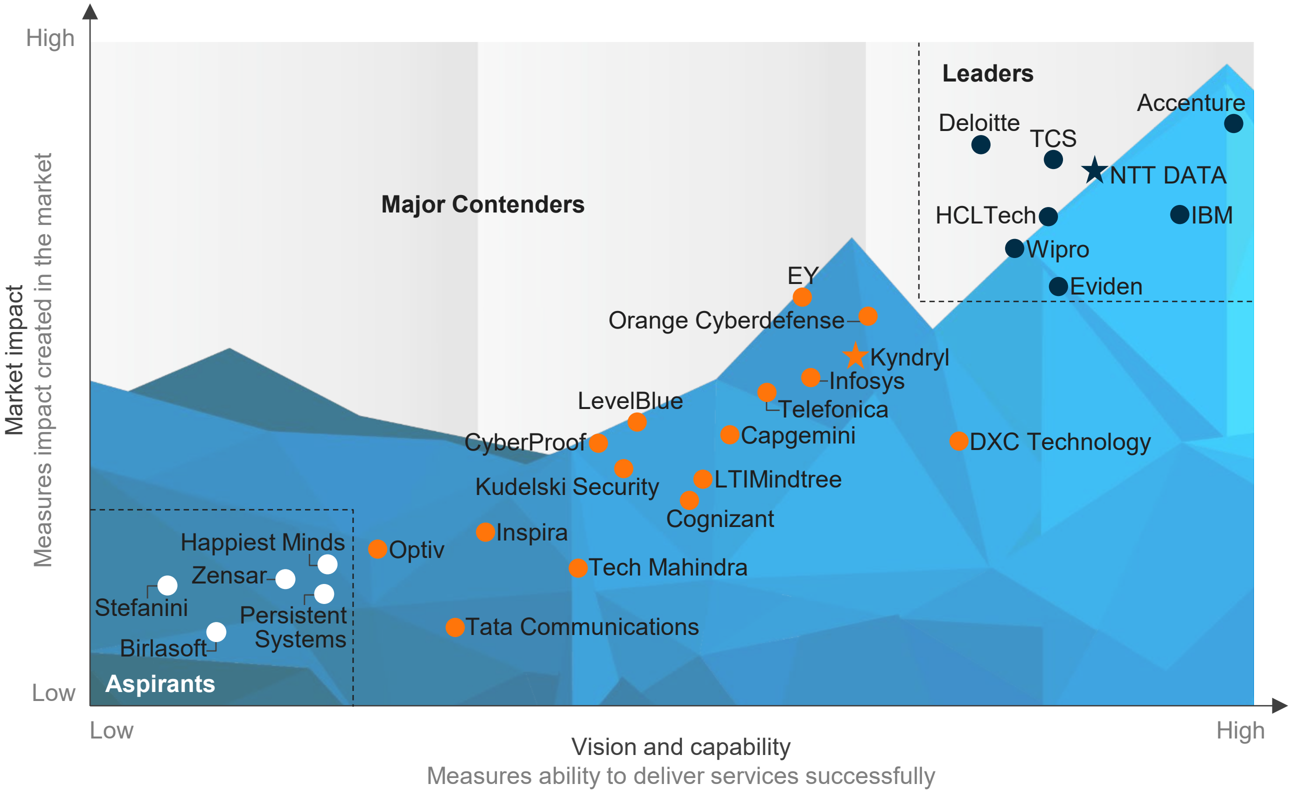
- Aspirants in the MDR market operate in niche areas and focus on addressing specific client needs, typically in small and mid-market segments
- These providers are in the early stages of developing their MDR capabilities and lack the scale to cater to large or global clients effectively
- Despite their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

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

NTT DATA profile (page 1 of 6)

Overview

Vision

NTT DATA's vision is to become a leading global cybersecurity company, with key emphasis on three main aspects. First, it aims to establish itself as a global leader with a significant market share and capabilities, setting high standards in cybersecurity. Second, it wants to provide consistent, high-quality services across all regions, ensuring multinational clients receive reliable security measures. The third aspect focuses on offering integrated services through a single company, allowing clients to access a comprehensive solution that combines the better offerings from various vendors, all managed by NTT DATA. Its goal is to support the provision of MDR services, maximizing the value delivered to customers as a trusted business partner.

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	◔ Latin America	◔ Middle East and Africa
○ Rest of the world		

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

● BFSI	◔ Energy and utilities	◑ Manufacturing
○ Electronics, hi-tech, and technology	◔ Healthcare and life sciences	◑ 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)

NTT DATA profile (page 2 of 6)

Case studies

CASE STUDY 1

Addressed vulnerabilities and enhanced security across operations

Client: A major Japanese beverage manufacturer

Business challenge

The client faced a surge in cyberattacks due to global instability including the COVID-19 pandemic and geopolitical tensions such as the conflict in Ukraine. Vulnerabilities within the client's subsidiaries and supply chain led to significant damage. As the business expanded internationally, it needed to improve defenses against these rising cyber threats and strengthen its overall cybersecurity governance to mitigate risks.

Solution and impact

- Implemented robust security measures including privacy data protection, global security visualization, and the creation of a Security Operation Center (SOC) as well as a Computer Security Incident Response Team (CSIRT)
- Collaborated with NTT DATA to accelerate global security enhancements, focusing on infrastructure and application development
- Established three pillars for strengthening security: reformulated governance policies and security rules, introduced tools for early attack detection, and improved employee security literacy through training programs

Key benefits

- Improved defense and response capabilities, ensuring business continuity and protecting the brand from potential damage
- Improved targets and addressed weaknesses identified during initial assessments

CASE STUDY 2

Addressed cybersecurity challenges and improved operational security

Client: A global manufacturing giant

Business challenge

The client faced challenges in protecting assets, reputation, and critical manufacturing lines. It needed a business partner to manage cybersecurity operations including protection, response, and recovery. Its previous services were siloed and reactive, lacking the capability to validate responses and protections before attacks occurred. Additionally, legacy processes were mostly manual and unstructured, making it difficult to ensure effective cybersecurity measures were in place.

Solution and impact

- Consolidated dedicated MDR, Security Information and Event Management (SIEM), endpoint, and vulnerability functions
- Delivered a comprehensive identity practice that included Identity and Access Management (IAM), Privileged Access Management (PAM), Public Key Infrastructure (PKI), and Identity Governance and Administration (IGA)
- Applied architecture, engineering, and automation specialists throughout the entire security program
- Developed a service roadmap that enhanced MDR services with leading SOAR, threat intelligence, and security validation tools

Key benefits

- Enabled faster and more accurate detection, response, and mitigation of threats
- Replaced ITIL Service Level Agreements (SLAs) with CSIRT protocols
- Established continuous direct validation of the effectiveness of security detection, response, and protection capabilities
- Enhanced protection and recovery capabilities to ensure critical manufacturing processes remained operational

NTT DATA profile (page 3 of 6)

Solutions

[REPRESENTATIVE LIST]

Proprietary MDR services solutions

Solution	Details
NTT DATA’s Security Sensor	It involves collecting log data and security signals from the client's network at standard, medium, and premium levels. The log data is analyzed onsite using AI, with security alerts sent back to the SOC. It utilizes an advanced architecture with caching and load balancing to ensure that no data is lost. Log collection achieved a 99.99% message retention rate.
NTT DATA Argus	It provides an analysis and detection service for unauthorized access monitoring. The service included analysis for attacks, unauthorized access, intelligence provision, notifications, reporting, and quality assurance responses based on customer system information. It adhered to Security Service Standards certified by the Ministry of Economy, Trade, and Industry in Japan and excluded 99.999% of false positives.
zenMDR	It offers a single point of access for SOC operators. The platform comprised multiple components, integrating both custom applications and commercial software. It is hosted on ISO 27001-certified infrastructure, and provides comprehensive MDR services for small, midsized, and large enterprises.
GxDR	It supports all areas of Extended Detection and Response (xDR) by enabling global SOC services for local customers, featuring unique capabilities for detection, prevention, and response. All activities were managed by operators within a single console that handled various tasks and information including threat intelligence, Endpoint Detection and Response (EDR), mail security, identity management, Configuration Management Database (CMDB) integration, and runbooks. The solution is hosted on ISO 27001-certified infrastructure and significantly enhances local operational capabilities with a high-quality, low-cost offering.
Rock^3	It collects log data and security signals from the client's network at standard, medium, and premium levels. The log data is analyzed onsite using AI, with security alerts sent back to the SOC. It employs an advanced architecture that utilizes caching and load balancing to ensure no data loss, achieving 99.999% availability.
UMDR	It is a next-generation managed security solution aimed at rapidly detecting and responding to security threats within customer environments. The service leverages accumulated expertise in security operations and incident response to enhance global security governance. For UMDR, a security service infrastructure called SOC Solutions is established to improve security operations, combining open-source tools and enterprise security services to support operational teams.
Nucleus Security Insights	It provides unified monitoring of antivirus, vulnerability scans, and security monitoring (SIEM) to protect clients' digital operations. It offers security insights on a unified platform, visualizing a comprehensive set of operational dashboards that deliver deep insights and context regarding infrastructure security including assets, antivirus status, vulnerabilities, and security monitoring.

NTT DATA profile (page 4 of 6)

Partnerships

[REPRESENTATIVE LIST]

Partnerships

Partner	Type of partnership	Details
CrowdStrike	Technology partnership	It partnered with CrowdStrike to resell a full range of services including MDR, incident response, consulting, and implementation through a packaged MSP engagement license program.
Microsoft	Technology partnership	NTT DATA partnered with Microsoft to develop MDR services that focus on quickly detecting and effectively responding to cybersecurity threats. This service integrated the capabilities of EDR technology, including Microsoft Defender for Endpoint, along with NTT's Network Detection and Response (NDR) technology, the Cyber Threat Sensor. The collaboration combined network and endpoint coverage with proprietary advanced analytics, global threat intelligence, and expert-driven threat hunting.
PaloAlto Networks	Technology partnership	It partnered with Microsoft to plan the launch of a MDR service offering based on Cortex XSIAM. This joint offering also integrated NTT Ltd.'s secure by design services with Palo Alto's Prisma™ Access and Cortex™ XSOAR technologies. The collaboration emphasized intelligent workplace, infrastructure, and cybersecurity solutions, allowing clients to secure complex, services-oriented IT environments.
Securonix	Technology partnership	NTT DATA partnered with Securonix and signed a Managed Security Service Provider (MSSP) agreement to enhance MDR services. It enhanced the global MSSP and MDR program by launching Securonix Fuel, aimed at accommodating record demand and accelerating growth.
Qualys	Technology partnership	It partnered with Qualys and provided Value Added Resellers (VARs) and Managed Service Providers (MSPs) with enhanced opportunities. It also implemented a channel partner program designed to support security-focused VARs, MSPs, and Managed Security Service Providers (MSSPs), offering access to the Qualys cloud platform and over 20 IT, security, and compliance applications.
Elastic Search	Technology partnership	NTT DATA partnered with Elastic Search as a resell and managed service partner to enhance MDR services.
Servicenow	Technology partnership	It partnered with ServiceNow and addressed the challenges faced by organizations with internal teams managing ServiceNow platforms. NTT DATA's ServiceNow managed services focused on effectively operating these environments, ensuring maintenance, deploying new releases, and managing day-to-day operational tasks.
Exabeam	Technology partnership	NTT DATA strengthened its MDR capabilities by partnering with Exabeam for advanced SIEM and behavioral analytics, enhancing threat detection and response.
Splunk	Technology partnership	It partnered with Splunk as a Global Strategic Integrator (GSI) partner, expanding its reach through VARs and MSPs depending on the country.
Swimlane	Technology partnership	NTT DATA enhanced its MDR services by partnering with Swimlane to leverage low-code security automation for improved threat response and efficiency.
Cyfirma	Technology partnership	It expanded its MDR capabilities by partnering with Cyfirma to integrate threat intelligence and attack surface management for proactive cyber defense.

NTT DATA profile (page 5 of 6)

Investments and recent activities

[REPRESENTATIVE LIST]

Investments and recent activities

Theme	Details
Investments	It developed global internal investments aimed at creating assets such as standardized architecture, automation and orchestration frameworks, and a consistent approach to incident response. This development allowed customers to select from a broader portfolio of services delivered uniformly. Additionally, customers could combine various services provided from different regions, enhancing flexibility and options for operational needs.
Innovation	It identified and tested new solutions and technologies globally through funded programs, evaluating vendors from both business and technical perspectives. Funding facilitated the execution of Proof-of-concepts (PoCs) with new technologies at existing customer sites, adhering to a standardized process to deliver comparable results. This initiative involved assessing and integrating new technology into existing offerings and services, as well as creating new solutions.
Alliances	It announced a global strategic partnership with CYFIRMA to enhance cybersecurity capabilities by shifting defense strategies from reactive to predictive. By leveraging CYFIRMA's DeCYFIR platform, organizations gained tools for proactive threat identification and monitoring. This collaboration aimed to improve risk mitigation and provide enterprises with real-time insights into potential vulnerabilities.
Alliances	It expanded its FOCUS partner program in collaboration with Claroty and added several MSSPs including IBM, Rockwell Automation, NTT DATA, and eSentire. This initiative aimed to enhance security posture and reduce risk across the Extended Internet of Things (XIoT) by leveraging specialized cybersecurity expertise.
Center of Excellence (CoE)	It established the Global Automotive Security Test Center in collaboration with C2A Security and Marelli to conduct AI-driven security tests for connected vehicles. This initiative aimed to enhance cybersecurity in software-defined vehicles by implementing agile security life cycles and adhering to regulations such as WP.29 and ISO 21434.
Trainings/Certifications	It developed a program aimed at increasing the number of cybersecurity professionals globally, announced a new global cybersecurity strategy. Following this, the first global cybersecurity talent development program was launched internally in January 2024 to foster expertise within the organization.
Innovation	It developed an SBOM Management asset through global investment, aimed to enhance clarity around software compositions of Open-source Software (OSS) and assess vulnerabilities. This initiative focused on providing both internal and client-facing solutions to strengthen software security and compliance.
Others	It enhanced the value of the Unified Managed Detection and Response (UMDR) service globally, released at the end of FY23, by leveraging CERT expertise and reducing operational costs through R&D achievements. Advanced operational technologies utilized AI for managed security service operations, aiming to improve efficiency and effectiveness in service delivery.

NTT DATA profile (page 6 of 6)

Everest Group assessment – Leader and Star Performer

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 extensive global SOC coverage will benefit from NTT DATA's network of 40+ SOC locations across multiple continents, with particularly strong presence in Japan, India, and Europe
- Enterprises seeking integrated security solutions can benefit from NTT DATA’s DFIR and Threat Intelligence Platform integration, enhancing MDR with faster detection and streamlined response
- Enterprises seeking network-level MDR can benefit from NTT DATA's proprietary Security Sensor technology for comprehensive log data and security signal collection
- Enterprises requiring extensive IT/OT telemetry coverage will benefit from NTT DATA's robust OT security partnerships and seamless integration of OT security logs into MDR services
- Enterprises seeking flexible engagement models benefit from NTT DATA's diverse pricing structure, supporting per-endpoint, per-user, fixed-fee, and hybrid models

Limitations

- Enterprises requiring expertise in the retail, distribution and CPG, or healthcare and life sciences verticals should carefully consider NTT DATA as it has limited delivery proof points for these verticals
- Clients anticipate NTT DATA to be more proactive in positioning innovative and cutting-edge solutions to address their evolving needs
- Enterprises focusing on emerging add-on MDR services such as breach and attack simulation and dark web monitoring might find NTT DATA’s limited focus in these areas limiting
- Some clients have pointed out that NTT DATA’s response times are slow, particularly during night-time monitoring
- Clients have raised concerns about operational efficiency of NTT DATA’s MDR services

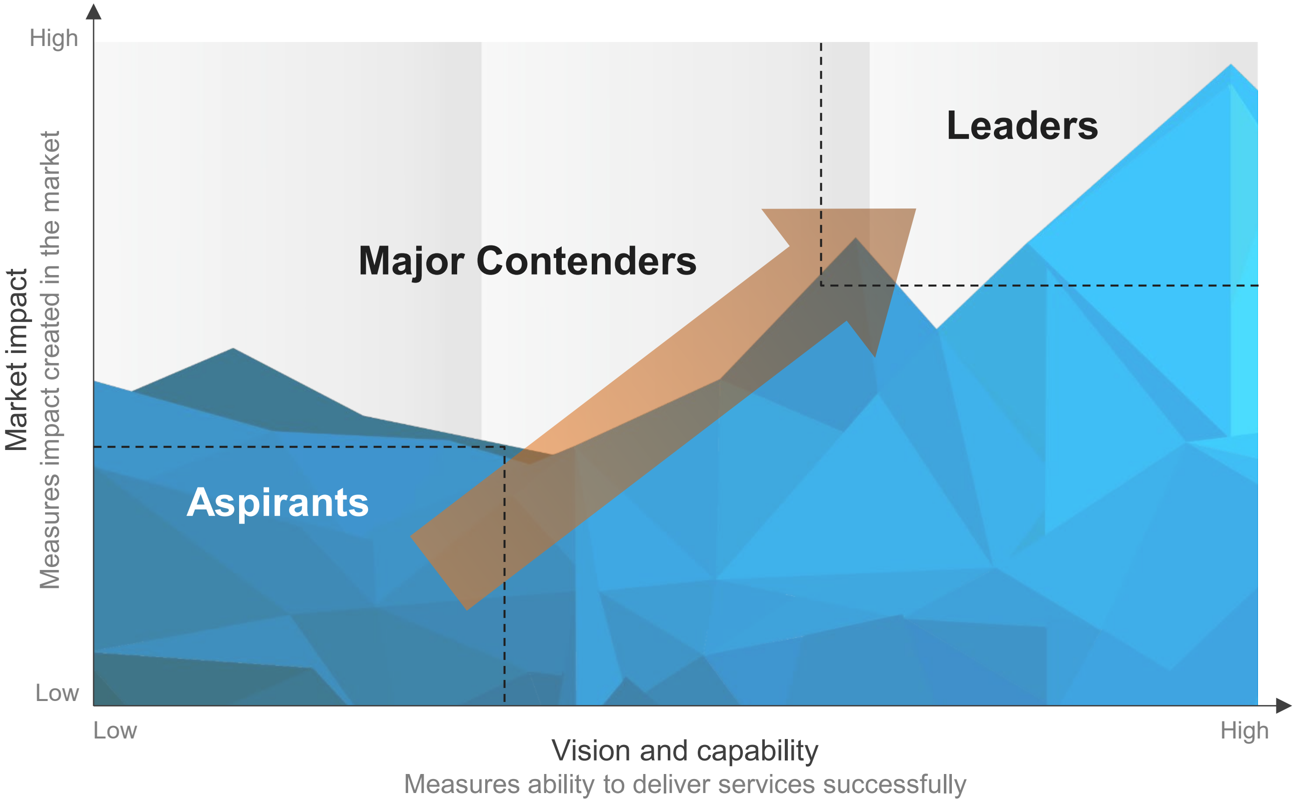
Appendix

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

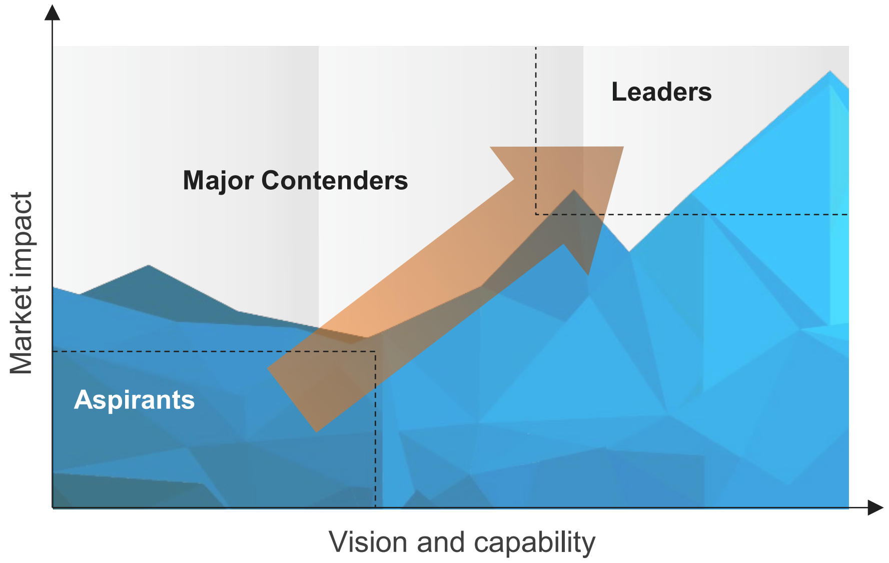
Services PEAK Matrix® evaluation dimensions

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

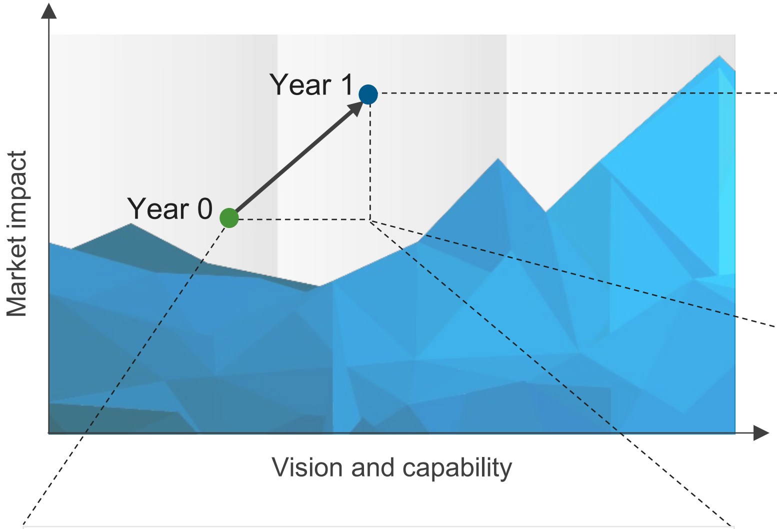
Innovation and investments
Innovation and investment in the enabling areas, e.g., technology IP, industry/domain knowledge, innovative commercial constructs, alliances, M&A, etc.

Delivery footprint
Delivery footprint and global sourcing mix

Everest Group confers the Star Performer title on providers that demonstrate the most improvement over time on the PEAK Matrix®

Methodology

Everest Group selects Star Performers based on the relative YoY improvement on the PEAK Matrix



In order to assess advances on **market impact**, we evaluate each provider's performance across a number of parameters including:

- Yearly ACV/YoY revenue growth
- # of new contract signings and extensions
- Value of new contract signings
- Improvement in portfolio mix
- Improvement in value delivered

In order to assess advances in vision and capability, we evaluate each provider's performance across a number of parameters including:

- Innovation
- Increase in scope of services offered
- Expansion of delivery footprint
- Technology/domain-specific investments

We identify the providers whose improvement ranks in the top quartile and award the Star Performer rating to those providers with:

- The maximum number of top-quartile performance improvements across all of the above parameters

AND

- At least one area of top-quartile improvement performance in both market success and capability advancement

The Star Performer title relates to YoY performance for a given provider and does not reflect the overall market leadership position, which is identified as Leader, Major Contender, or Aspirant.

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