



Everest Group PEAK Matrix[®] for Managed Detection and Response (MDR) Services Provider 2023

Focus on Accenture
December 2022



Background of the research

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) 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 full 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

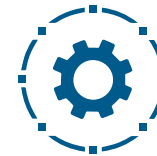
Scope of this report



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:

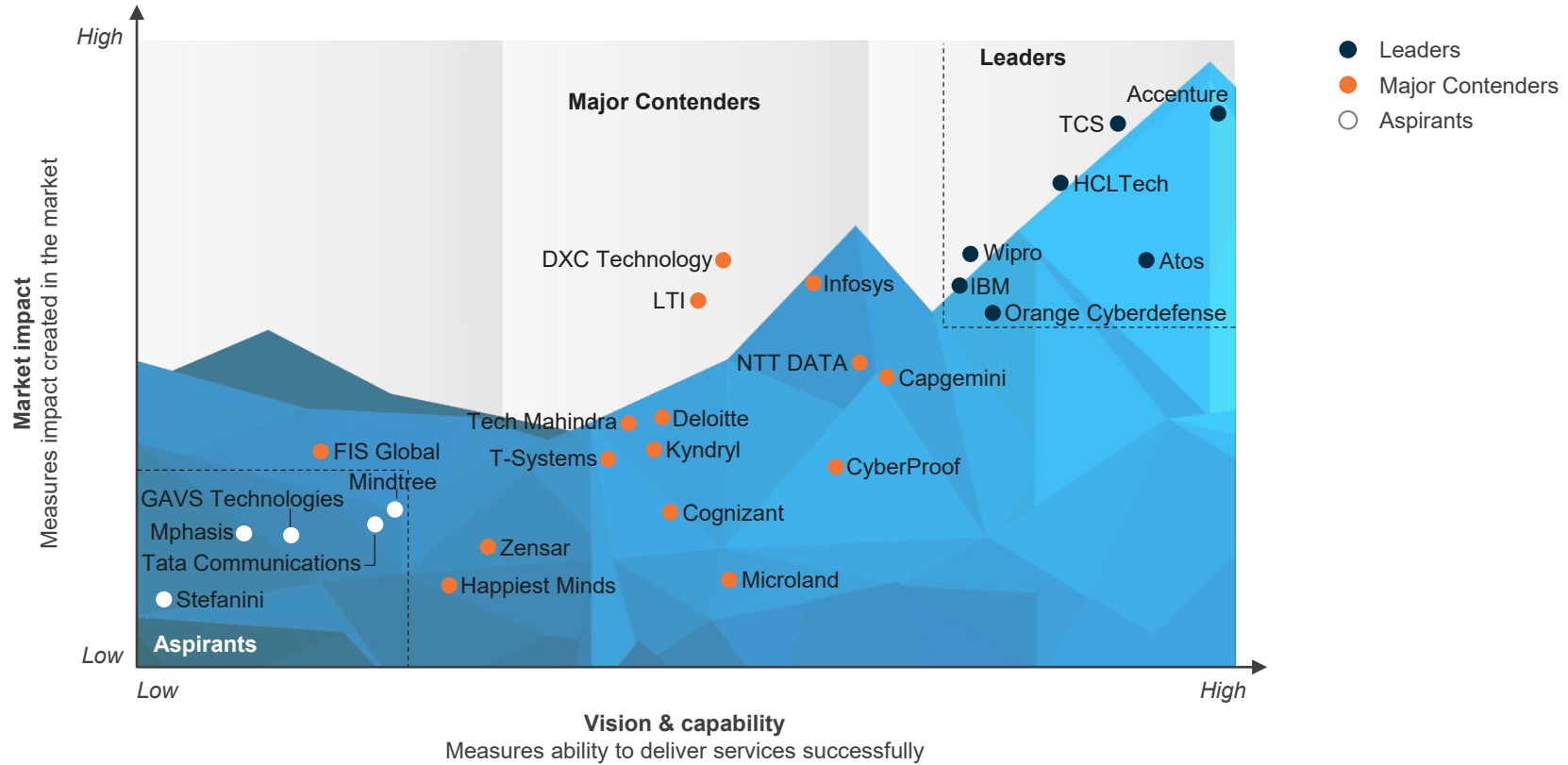
GAVS Technologies, Mindtree, Mphasis, Stefanini, and Tata Communication

- 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) PEAK Matrix® Assessment 2022 | Accenture 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)

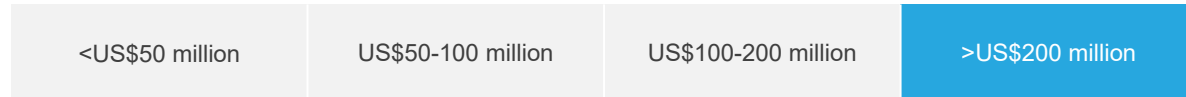
Accenture | MDR services profile (page 1 of 7)

Overview

Company mission/vision statement

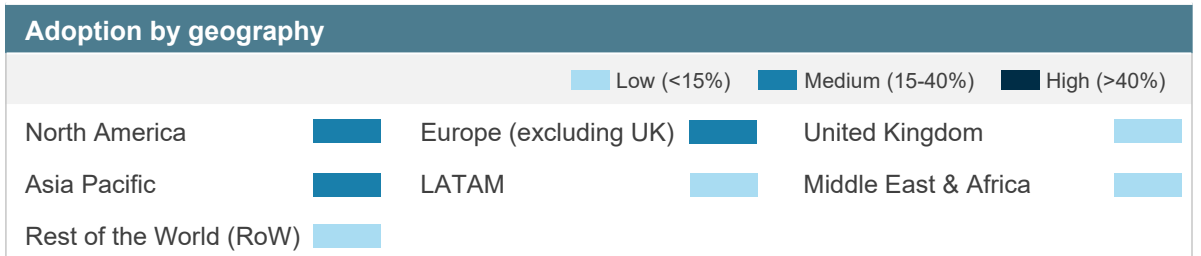
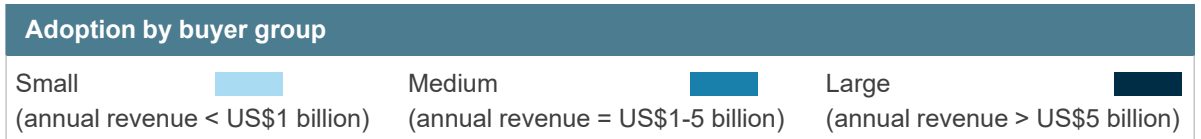
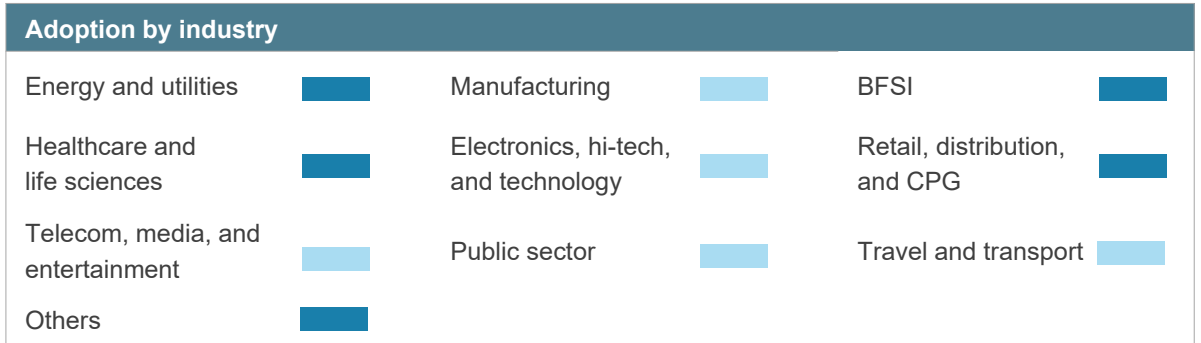
Accenture aims to be the world's leading managed detection and response services partner by prioritizing the security needs of its clients. It aids customers in their journey by providing them with cutting-edge detection and response services and a cybersecurity talent pool, all of which are designed to provide innovation, adaptability, and scalability for MDR services.

MDR services revenue (2021)



NOT EXHAUSTIVE

Low (<10%) Medium (10-20%) High (>20%)



Accenture | MDR services profile (page 2 of 7)

Case studies

Case study 1

Responding to ransomware with MxDR

Client: a large manufacturing company

Business challenge

The client suffered a ransomware attack and discovered that it did not have coverage or the technical competence to remediate it. It sought Accenture's assistance. The coverage was limited since the existing provider's pricing approach was dependent on log ingest. To that aim, the client opted to pick and choose which logs to deliver. Given the repercussions of the ransomware assault, this proved to be even more costly in the end. As a result, the client was unsatisfied and apprehensive about the restricted coverage.

Solution

Accenture's Managed Extended Detection and Response (MxDR) solution gave the client a full suite of capabilities, with end-to-end coverage for cloud, network, end-point, and SaaS applications – including OT and IoMT environments – 24x7 monitoring, 1,000+ out-of-the-box detections, and pre-authorized actions on the end-point. The client also engaged the Cyber Investigations, Forensics, & Response (CIFR) team to help contain any spillage from the ransomware attack.

Key benefits

Through Accenture's MxDR, the client received the following services:

- Lower Total Cost of Ownership (TCO) by combining people and technology, removing the burden of buying and maintaining technology and retaining talent
- Better Return on Investment (RoI) and easy prediction of cost by maximizing security investment by remaining vendor-agnostic, avoiding costly rip-and-replace business models
- Low noise, high fidelity, and immediate detection capability as it combines analytics engines and 1,000+ out-of-the-box use cases

Case study 2

Postal service leapfrogged into the future leveraging Accenture's automation and orchestration expertise

Client: a multinational postal service and courier company

Business challenge

As part of the cloud journey, the client sought a security partner to provide the next generation of security monitoring, automation, and incident response services. The client's main priority was to secure its end-to-end supply chain, OT, and IT systems, especially in light of escalating assaults on national infrastructure.

Solution

Accenture helped the client by incorporating automation and orchestration into the core service and delivering Machine Learning (ML) in threat detection. Accenture doubled the security coverage of the previous provider through a collaborative solution developed with Microsoft.

Further, it leveraged the Microsoft Cloud-based (Azure and Sentinel) platform for threat hunting, enabling proactive detection and mitigation of cyber threats, raising the maturity level of the client's SOC, and providing recommendations for targeted threat intelligence and penetration testing.

Key benefits

The solution enhanced the client's cloud security posture and delivered the following benefits:

- Exhibited cost-effective requirements by implementing Microsoft Sentinel for the client's security monitoring
- Leveraged the latest advances in cloud security monitoring, detection, and automated response at one of the most critical times for its business

Accenture | MDR services profile (page 3 of 7)

Solutions

Proprietary solutions (representative list)

Solution name	Details
Service – Managed Extended Detection & Response (MxDR)	Full suite detection, response, and remediation – including people, platform, licenses, and storage – to proactively mitigate cyber attacks and malicious activity at a lower price point
Service – Managed SIEM and SOAR	Real-time monitoring, detection, and response based on the client's SIEM platform and supported by SOAR (Accenture-hosted or client-owned), including platform management. It includes Splunk, Microsoft Sentinel, IBM Qradar, Google Chronicle, Exabeam, LogRhythm & Splunk Phantom, Palo Alto XSOAR, and Microsoft Logic Apps
Service – Managed EDR	End-to-end management, including policy maintenance, threat monitoring, and response, leveraging the client's EDR platform. It includes Microsoft Defender, Carbon Black, CrowdStrike, Endgame, and Palo Alto Cortex
Service – MDR for OT/IoT/IoMT	Critical threat detection across general IoT, medical, and operational technology environments leveraging both monitoring toolsets and threat intelligence for industry-/environment-specific use cases. It is available both with MxDR and Managed-SIEM
Service – MDR for Salesforce	Critical threat detection via custom analytics across client Salesforce deployments, built around native Salesforce logging
Service – MDR for SAP	Critical threat detection via custom analytics across client SAP deployments, built around native SAP logging
Service – Intelgraph intelligence portal and API	Accenture's IntelGraph intelligence portal combines context-rich reports, powerful visualizations, advanced searching, alerting, and a robust RESTful API to enable faster access to relevant threat data and allow efficient and easy pivoting on threat indicators.
Service – incident response retainer	Offers 24x7 global incident response capability with deep specializations across incident response, forensics, OT, and Cloud (two-hour response SLA)
Asset – Accenture delivery methods and estimators for security	Accenture Delivery Methods (ADM) for security provide delivery methods for common security planning and security implementation services. Estimators are available to plan and deliver large-scale, complex consulting/assessment, design/integration, and outsourcing programs.
Asset – content library	A use case library with advanced detections & response capabilities, including SOAR playbooks, curated & maintained by its Global Intelligence Operations (GIO) team for the entire client base with content tailored by the industry.
Asset – mySecurity.Posture	Automated MITRE ATT&CK-based assessment that provides transparency around a client's security gaps, highlighting areas of improvement based on known adversary behaviors
Asset – CIFR react	Massively scalable incident response evidence collection and analysis platform utilizing Accenture's threat intelligence and behavioral detections library
Asset – recon darknet detection	An asset-based, automated solution designed to monitor and measure risks and impact on a client's attack surface. It is used to consistently identify existing threats directly relevant to clients' businesses as well as uncover new and emerging threats that clients use to improve their respective security postures.

Accenture | MDR services profile (page 4 of 7)

Partnerships

Partnerships (representative list)		
Partner name	Type of partnership	Details of the partnership
AWS	MDR partnership	Strengthen the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)
Carbon Black	MDR partnership	Detect, respond to, and recover from threat actors and breaches impacting business operations
CrowdStrike	MDR partnership	Detect, respond to, and recover from threat actors and breaches impacting business operation.
Elastic	MDR partnership	Data enhancement and visualized analytics that allow clients to create pivot tables, nested queries, and visualizations based on their log data
Forescout	MDR partnership	Secure connected devices (IoT/IIoT/ICS) and embedded systems to enable intelligent, connected, and trusted products and services for clients' use internally and to sell to their customers; this includes securely building, implementing, and operating SW & HW
Google	MDR partnership	Strengthens the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)
Microsoft	MDR partnership	Strengthens the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)
Nozomi	MDR partnership	Secure connected devices (IoT/IIoT/ICS) and embedded systems to enable intelligent, connected, and trusted products and services for clients' use internally and to sell to their customers. This includes securely building, implementing, and operating SW & HW
Palo Alto Networks	MDR partnership	Deployed XSOAR across its delivery centers in Europe unifying automation, case management, real-time collaboration, and threat intelligence management. Protecting core enterprise applications such as ERPs, CRMs, and other critical business platforms by hardening environments and improving monitoring, security testing, governance, and risk and compliance
Prevailion	MDR partnership	A next-generation cyber intelligence company that provides expansive visibility into malware through adversary counterintelligence; this partnership enhances Accenture's ability to provide advance warning of cyber threats that could potentially compromise clients' systems and third-party ecosystems.
SAP	MDR partnership	Security monitoring across SAP deployments, without the need to deploy any additional tooling
Salesforce	MDR partnership	Security monitoring across Salesforce deployments, without the need to deploy any additional tooling
Splunk	MDR partnership	Cyber defense security transformation, SIEM services, and managed security services
Zscaler	MDR partnership	Strengthen the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)
Vodafone	MDR business partnership	Strategic partnership to deliver world-class managed security services to SMBs across Europe

Accenture | MDR services profile (page 5 of 7)

Partnerships

Partnerships (representative list)		
Partner name	Type of partnership	Details of the partnership
Fortinet	Technology partnership	Secure connected devices (IoT/IIoT/ICS) and embedded systems to enable intelligent, connected, and trusted products and services for clients' use internally and to sell to their customers; this includes securely building, implementing, and operating SW & HW
Micro Focus	Technology partnership	Application security scanning, managed security services, SIEM services, and application security services
Okta	Technology partnership	Design and implement Identity and Access Management (IAM) services capable of securing client environments and experiences
ServiceNow	Technology partnership	Transform governance, risk & compliance, and integrated risk management processes, taxonomy, and reporting through technology enablement
VMWare	Technology partnership	Detect, respond to, and recover from threat actors and breaches impacting business operations

Accenture | MDR services profile (page 6 of 7)

Investments and recent activities










Investments and recent activities (representative list)

Themes	Details
Acquisitions	Invested in acquiring nine companies to provide a full range of MDR services across clients' IT and OT systems. These acquisitions include the US federal government services business of Endgame Inc. (2017), iDefense (2017), Deja Vu Security (2019), Context Information Security (2020), Revolutionary Security (2020), Symantec Cybersecurity Services (2020), Real Protect (2021), Openminded (2021), and Sentor (2021).
Talent	<p>Accenture continues to invest in talent to upskill its employees in areas including cloud certifications from cloud service provider partners such as Microsoft Azure, AWS, GCP, Alibaba, VMware, Workday, Salesforce, and others.</p> <ul style="list-style-type: none"> • Security training and certification: programs to nurture employees in cybersecurity and soft skills such as ecosystem of social learning, analytics, and certifications including CISSP, CIPP, SABSA, CompTIA Security+, CompTIA CyberSec CSA, AWS, and many more • Security academy: Accenture has made considerable investments in a cutting-edge curriculum with over 2,500 learning assets to rapidly educate people and facilitate talent growth with comprehensive program specialists • Security professional community portal: Across Accenture, the site remains a top-ranked professional community. Deep industry, function, or technical knowledge and specialization-brings together material for over 14,000 colleagues and specialists • Non-STEM females training: Accenture, in cooperation with Pink Academy, offers eight-week training programs for female students with a humanistic/economic background who are eager to master security core skills in cloud security, cyber defense, data protection, and strategy & risk • Online Master of Science in cybersecurity (OMS cybersecurity): This is offered in collaboration with Georgia Tech's online Master of Science in Cybersecurity degree program to meet the demand for highly skilled cybersecurity professionals • Collaboration with universities: strong collaboration to create and attract talent, with Accenture professionals creating and delivering security classes to develop future experts that can join Accenture MDR teams directly or via an internship
Others	<ul style="list-style-type: none"> • Accenture cybersecurity forum: The forum has 300+ members, the majority of whom are CISOs from various industries, as well as CEOs and board members. It hosts monthly virtual roundtables on current problems as well as in-person events on a regular basis • Cyber labs: The labs focus on sensitive data discovery using machine learning, attack prediction via graph analytics, responsible AI, and application attack surface reduction • Cyber ranges: Controlled, interactive, and realistic environments, cybersecurity research, and MSS services focused on Industrial Control Systems (ICS) and Operational Technology (OT)

Accenture | MDR services profile (page 7 of 7)

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

- Accenture has invested in building its own MDR platform named MxDR, which allows it to offer more customization and extensive integration options for enterprise clients
- Enterprises can benefit from Accenture’s extensive investments in building its threat-hunting and threat-intelligence capabilities through six MDR-centric acquisitions in the last three years
- Enterprises will find Accenture attractive because of its delivery capabilities around converged IT-OT security services, backed by the OT-dedicated Cyber Fusion Centers (CFC) and sizable IT-OT partner ecosystem
- Enterprises looking for multi-language support will find Accenture to be relevant because of its ability to provide MDR support in 11 different languages
- Accenture will be a relevant choice for clients looking for flexible SOC engagement options because of Accenture’s dedicated, shared, and hybrid SOCs

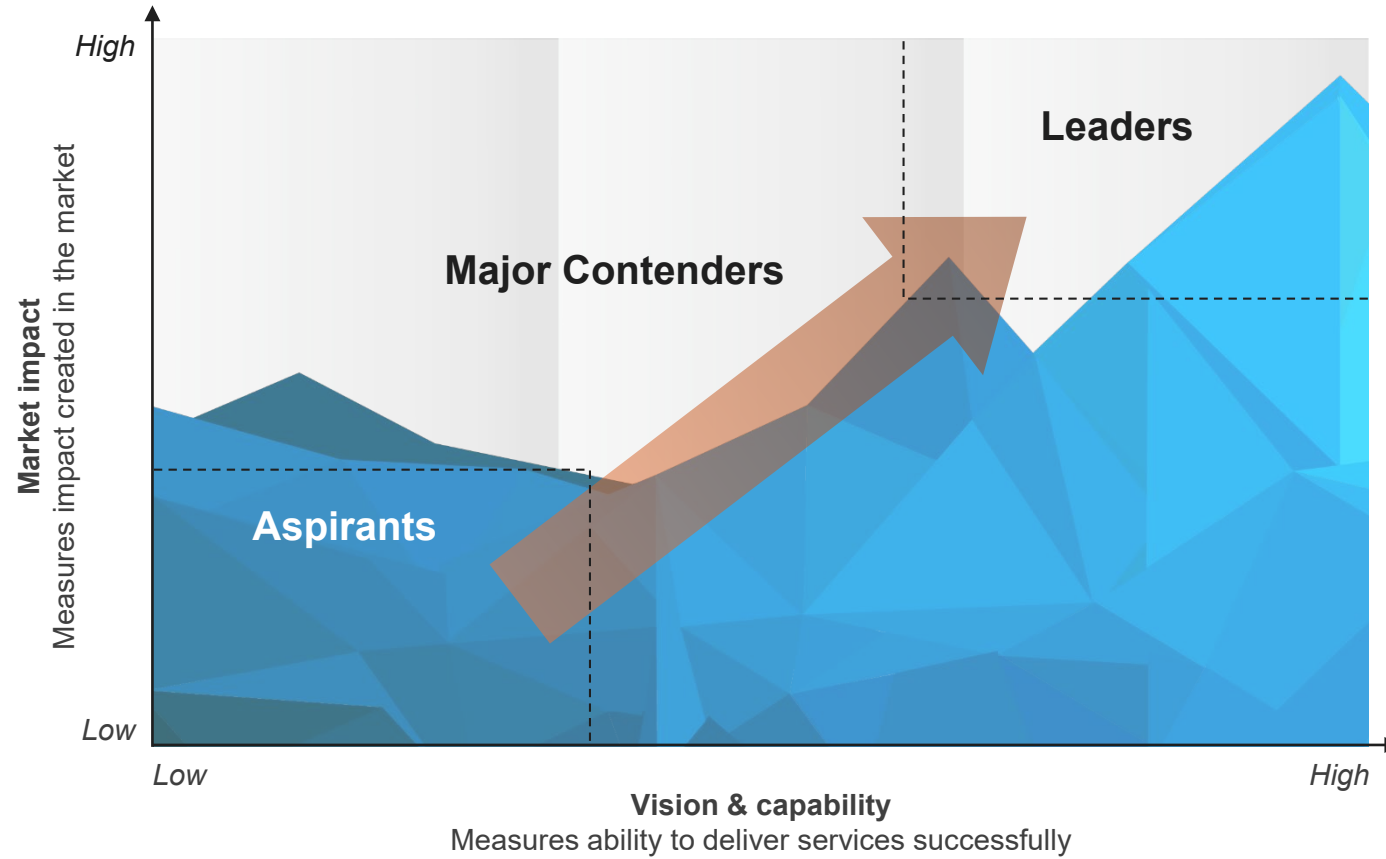
Limitations

- Clients have highlighted that Accenture can improve its log analytics capabilities from SentinelOne to enable high-fidelity alerts and better reporting
- Enterprises should be wary of Accenture’s comparatively lesser presence in industries such as BFSI, manufacturing, retail, distribution, and CPG
- Enterprises looking for higher onshore resource presence might find Accenture lagging compared to peers
- Small sized buyers need to be aware that Accenture is more focused on medium and large-scale clients for MDR services

Appendix

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

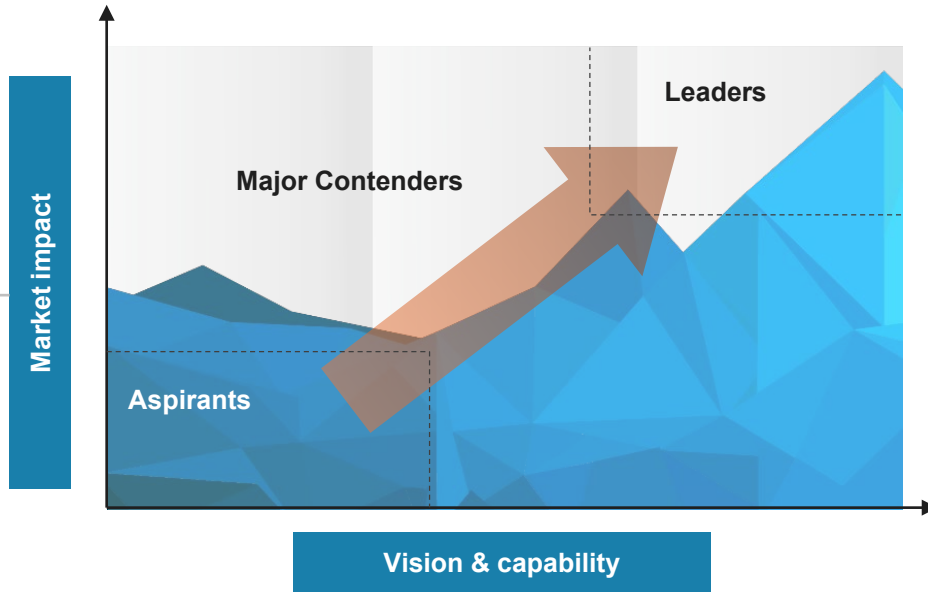
Everest Group PEAK Matrix



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

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 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 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.