

Everest Group PEAK Matrix® for IT Security Service Provider 2022 – North America

Focus on Accenture
August 2022



Background of the research

Organizations are leveraging IT security services to improve their security posture and prepare for challenges such as ransomware attacks and business disruptions. The COVID-19 pandemic has further accelerated the adoption of security services, buttressed by enterprise challenges, in securing a remote workforce. Another important factor that has significantly contributed to the rise of IT security services is the shortage of expert cybersecurity talent and rising CAPEX and OPEX in maintaining in-house security teams, especially during the great resignation period. The US federal government too has taken a serious stance against cybercriminals and has been proactive in making laws and issuing executive orders covering a wide variety of security challenges ranging from OT security to data privacy laws such as CCPA and GDPR. All these factors combined have resulted in a major uptick in IT security services demand across the North American geography.

In this research, we present an assessment and detailed profiles of 27 IT service providers for the IT security capabilities in the North American region featured on the [IT Security Services PEAK Matrix® Assessment 2022 – North America](#). The assessment is based on Everest Group’s annual RFI process for the calendar year 2022, interactions with leading IT security service providers, client reference checks, and an ongoing analysis of the IT security services market.

The full report includes the profiles of the following 27 leading IT security service providers featured on the IT Security Services PEAK Matrix – North America:

- **Leaders:** Accenture, HCL Technologies, IBM, TCS, and Wipro
- **Major Contenders:** AT&T, Atos, Capgemini, Cognizant, Deloitte, DXC Technology, EY, Infosys, KPMG, Kyndryl, LTI, Microland, Mphasis, NTT DATA, PwC, Tech Mahindra, and Zensar
- **Aspirants:** GAVS Technologies, Happiest Minds, ITC Secure, Mindtree, and Yash Technologies

Scope of this report



Geography
North America



Providers
27



Services
IT Security Services

IT security services PEAK Matrix® – North America characteristics

Leaders:

Accenture, HCL Technologies, IBM, TCS, and Wipro

- Leaders have gained significant mindshare among enterprise clients due to the depth and breadth of their IT security services portfolio and on-ground presence in the North American geography. These players have a strong focus on next-generation security themes such as zero-trust, security analytics, OT security, security-embedded portfolio, Secure Access Service Edge (SASE), and Identity and Access Management (IAM)
- These providers have a highly balanced portfolio and continue to keep pace with market dynamics through continued investments in next-generation security solutions and services capability development (internal IP/tools, partnerships, etc.)

Major Contenders:

AT&T, Atos, Capgemini, Cognizant, Deloitte, DXC Technology, EY, Infosys, KPMG, Kyndryl, LTI, Microland, Mphasis, NTT DATA, PwC, Tech Mahindra, and Zensar

- These players have built meaningful capabilities to deliver IT security services; however, their service portfolios are not as balanced and comprehensive as those of Leaders (either in terms of coverage across IT security service segments, delivery mix, service type, or all)
- All these providers are making continued investments in developing internal IP and tools as well as expanding their service and technology partner ecosystem to plug their capability gaps, and are, thereby, positioning themselves as strong challengers to Leaders in this space

Aspirants:

GAVS Technologies, Happiest Minds, ITC Secure, Mindtree, and Yash Technologies

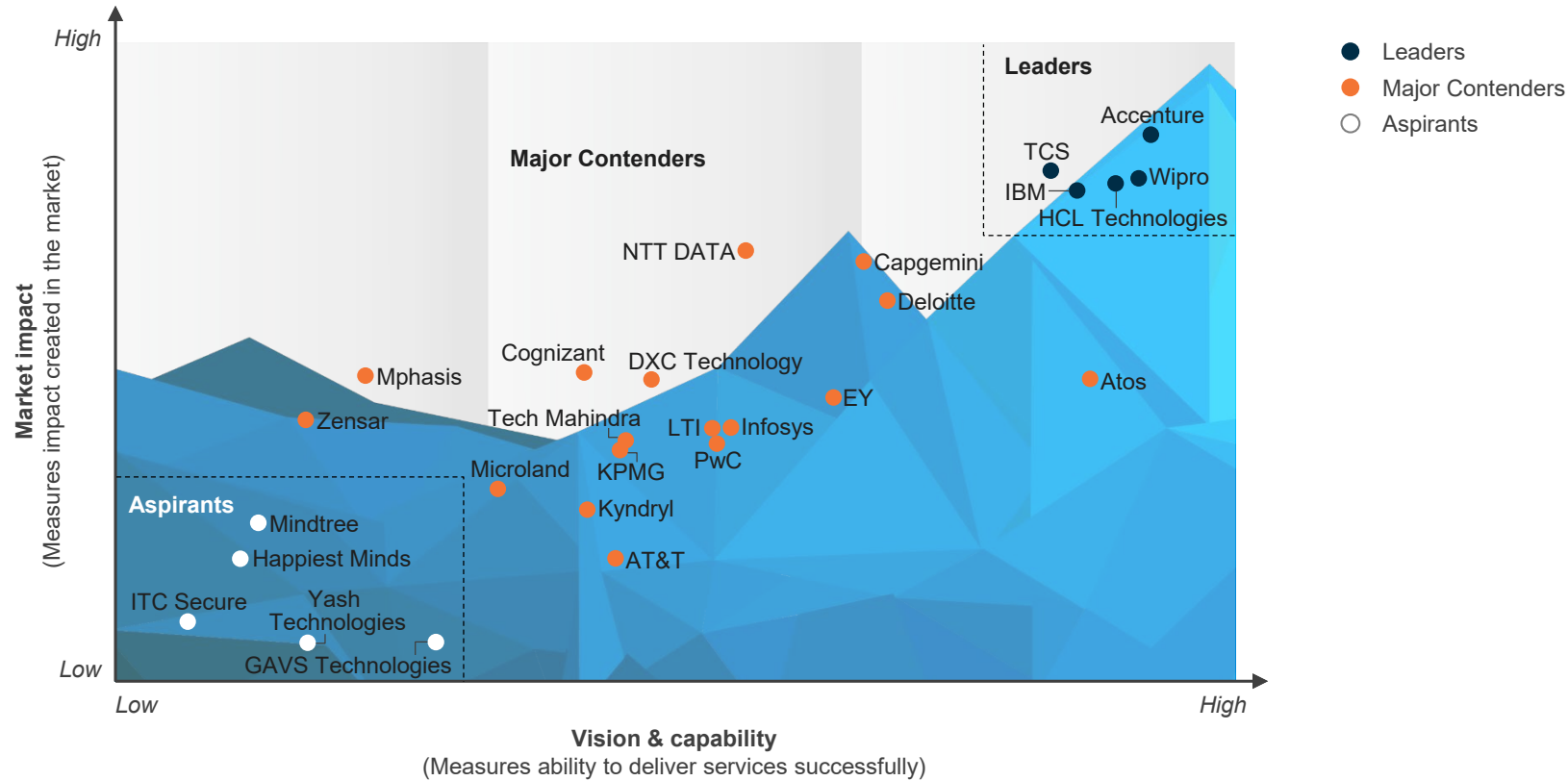
- The IT security services business of Aspirants is at a relatively early stage and is not a leading revenue generator for such players
- Nevertheless, these companies are making investments to build broader capabilities in the IT security services space to cater to buyers through service and technology partnerships as well as internal IP/tools – keeping them poised to be major challengers in the space

Everest Group PEAK Matrix®

IT Security Services PEAK Matrix® Assessment 2022 – North America | Accenture positioned as Leader



Everest Group IT Security Services PEAK Matrix® Assessment 2022 – North America^{1,2}












¹ Assessments for IBM, Capgemini, Deloitte, EY, KPMG, PwC, and AT&T 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 | IT security services – North America (page 1 of 6)

Everest Group assessment – Leader

Measure of capability:  Low  High

Market impact				Vision & capability				
Market adoption	Portfolio mix	Value delivered	Overall	Vision and strategy	Scope of services offered	Innovation and investments	Delivery footprint	Overall
								

Strengths

- Clients will benefit from Accenture’s comprehensive solution set that cuts across security themes such as OT security, application security, cloud security, IAM, and zero-trust; this is further enhanced by Accenture’s continued bolt-on acquisitions
- Enterprises looking to invest in next-generation security will find Accenture attractive due to its extensive investments in innovation and new-age solutions such as blockchain-based identities, connected car security, and digital twin security solution- CyTwin
- Accenture has baked in automation in its security services, resulting in reduced false alerts, faster threat detection, and faster security logs analysis for clients
- It has invested in cyber risk quantification for board-level executives, which provides a single pane view into cybersecurity RoI to board-level executives
- Clients have appreciated Accenture for its ability to deliver complex security engagements and its deep domain and technical expertise, and see it as a strategic partner in security

Limitations

- A few clients have raised concerns about Accenture’s high attrition in security service
- Despite being lauded by clients for its breadth of security offerings and its expertise, clients have raised concerns around its premium pricing and contractual flexibility
- Enterprise buyers looking for pure-play managed services might not find Accenture suitable as it has a relatively higher focus on consulting, design, and implementation-based projects for large enterprises
- A few clients have highlighted that Accenture needs to increase its presence in BFSI and manufacturing verticals

Accenture | IT security services – North America (page 2 of 6)

Overview

Vision

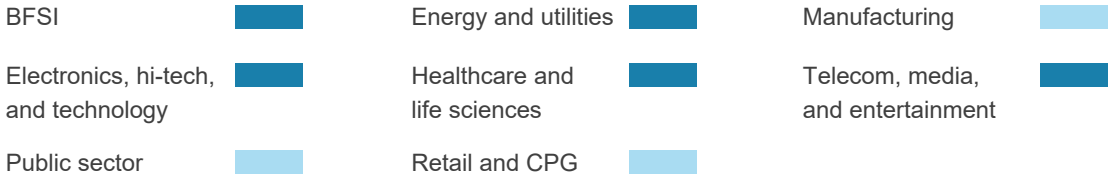
Accenture intends to provide a more secure environment for people and organizations to exist, by enabling enterprises to build an effective defense against known threats with the capacity to identify and respond to the unforeseen. It leverages next-generation security technologies and global resources to enhance security operations and better anticipate attacks, contain breaches, minimize vulnerabilities, and ensure business continuity. Further, with the intent to alleviate human capital challenges and shortages, Accenture strives to grow and train more security professionals with an emphasis on automation and AI.

IT security services revenue (2021)

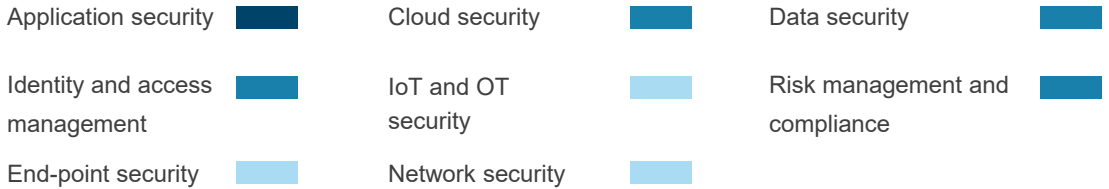


Low (<10%) Medium (10-20%) High (>20%)

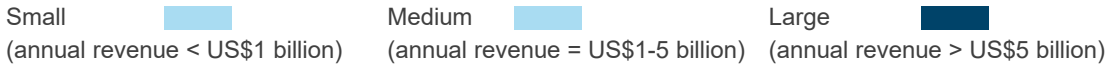
Adoption by industry



Adoption by service segments



Adoption by buyer group



Adoption by country

Low (<15%) Medium (15-40%) High (>40%)



Source: Everest Group (2022)

Accenture | IT security services – North America (page 3 of 6)

Case studies

Case study 1

Strengthen cybersecurity posture of a leading telecom player

Client: a telecom leader

Business challenge

The client desired to strengthen its security infrastructure in order to defend itself against cyber attacks such as SIM swaps.

Solution

Accenture pen-tested more than 1,000 applications and demonstrated what coordinated SIM swap attacks and device fraud looked like. Further, it conducted periodic scans as per the client’s new compliance policies, unearthing multiple vulnerabilities, offered risk-management insights from pen-testing, and assisted in the development of an in-house application to provide real-time reporting and transition the client into a new Splunk-based solution. To offer centralized visibility and a future-state security framework, the team integrated alerts with Enterprise Governance, Risk, and Compliance (EGRC).

Impact

- The client identified and mitigated over two million vulnerabilities and 30,000 critical or high-status threats
- The client discovered more than 170 million validated, unprotected, and sensitive data elements
- The solution improved data discovery and reduced US\$25 billion in breach risks cost
- The client has significantly reduced development costs by automatically identifying and disclosing security issues to developers before the code is written
- The client reduced work effort by 80% by implementing an application onboarding factor

Case study 2

Revamping cyber insurance supply chain using threat intelligence service to enhance accountability and efficiency in the market

Client: a global insurance provider

Business challenge

The client faced stiff competition in the cyber insurance market. Relying on a range of suppliers, its offering of disconnected services was providing limited value, necessitating the need to build a modern cyber insurance capability from the ground up.

Solution

Accenture assisted the insurer in envisioning a new cyber insurance relationship model that will serve clients across the policy life cycle. It integrated strategy and risk, iDefense, Fusion X, and insurance capabilities to assist insurers with risk assessments and threat intelligence evaluation throughout the sales process. Accenture negotiates new contracts for legal, public relations, and forensic accounting services and responds to incidents during the claims process to manage customers. In addition, it provides tailored training to the insurer’s workforce and engages in collaborative marketing operations.

Impact

- The insurer’s new end-to-end cyber insurance solution reduces the risk for the customers it covers, lowers cyber claim costs, generates higher revenues, and has a growing roster of new clients
- It has reduced claims collection expenditure to pay for pre-breach services
- Through its end-to-end cyber insurance, the insurer expects to further reduce cybercrime expenses

Accenture | IT security services – North America (page 4 of 6)

Solutions/IP/products

Proprietary solutions / IP / Products (representative list)	
Solution	Details
Autonomous Identity	A patented analytics and machine learning solution that analyzes enterprise access controls and makes recommendations; licensed/sold through partner ForgeRock
Cloud identity governance & administration accelerator	Modular, pre-built reference architectures, data models, and integrations to enable cloud-based Identity, Governance, and Administration (IGA) for large, highly complex organizations
Intelligent App Sec platform	A patented solution that enables secure application development at scale via auto-triage and auto-remediation solutions
Secure Cloud	Provides standardized strategy and repeatable IP, automation, and frameworks that are provided and installed into clients' cloud accounts to enable DevSecOps
Secure Platforms	IP and tooling for SAP, Oracle, and Salesforce to perform fast, consistent, and accurate security assessments
Accenture Delivery Methods (ADM) and estimators for security	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
Industry security value chains	Presents the key operational activities, processes, or products for each industry; critical assets, key threat actors, and sample threats are also identified
Recon darknet detection	An automated system to monitor and measure risks and impact to a client's attack surface; it identifies existing threats relevant to clients' businesses, uncovers new and emerging threats, and helps clients improve their security postures
RPA bot	A bot that utilizes intelligent automation via Robotic Process Automation (RPA) and Artificial Intelligence (AI) to respond to requests and enable autonomous identity user interchange, while reducing associated cyber threats

Accenture | IT security services – North America (page 5 of 6)

Partnerships

Partnerships (representative list)		
Partner	Partnership type	Details
AWS	Technology	Helps strengthen the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)
CrowdStrike	Technology	Partner for detect, respond to and recover from threat actors and breaches impacting business operations
CyberArk	Technology	Provide digital identity and privileged access management services
Forescout	Technology	Secure connected devices (IoT/IIoT/ICS) and embedded systems to enable intelligent, connected, and trusted products and services for clients' use internally and for their customers; this includes securely building, implementing, and operating SW and HW
ForgeRock	Technology	Provide digital identity and autonomous identity services
Google	Technology	Helps strengthen the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)
Micro Focus	Technology	Provide application security scanning, managed security services, SIEM, and application security services
Microsoft	Technology	Helps strengthen the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)
Nozomi Networks	Technology	Secure connected devices (IoT/IIoT/ICS) and embedded systems to enable intelligent, connected, and trusted products and services for clients' use internally and for their customers; this includes securely building, implementing, and operating SW and HW
Okta	Technology	Provide a solution for the design and implementation of IAM services
One Identity	Technology	Provide an IGA solution and Identity Manager of IAM services
Palo Alto Networks	Technology	Protect 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
SailPoint	Technology	Leverage IAM services capable of IdentityIQ and open identity platform
Saviynt	Technology	Design and implement 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
Splunk	Technology partnership	Cyber defense security transformation, SIEM services, and managed security services
VMWare	Technology partnership	Detect, respond to, and recover from threat actors and breaches impacting business operations
Zscaler	Technology partnership	Strengthen the ability to detect, prevent, and respond to infrastructure threats (networks, clouds, endpoints, mobile, and IoT)

Accenture | IT security services – North America (page 6 of 6)

Investments, and recent activities

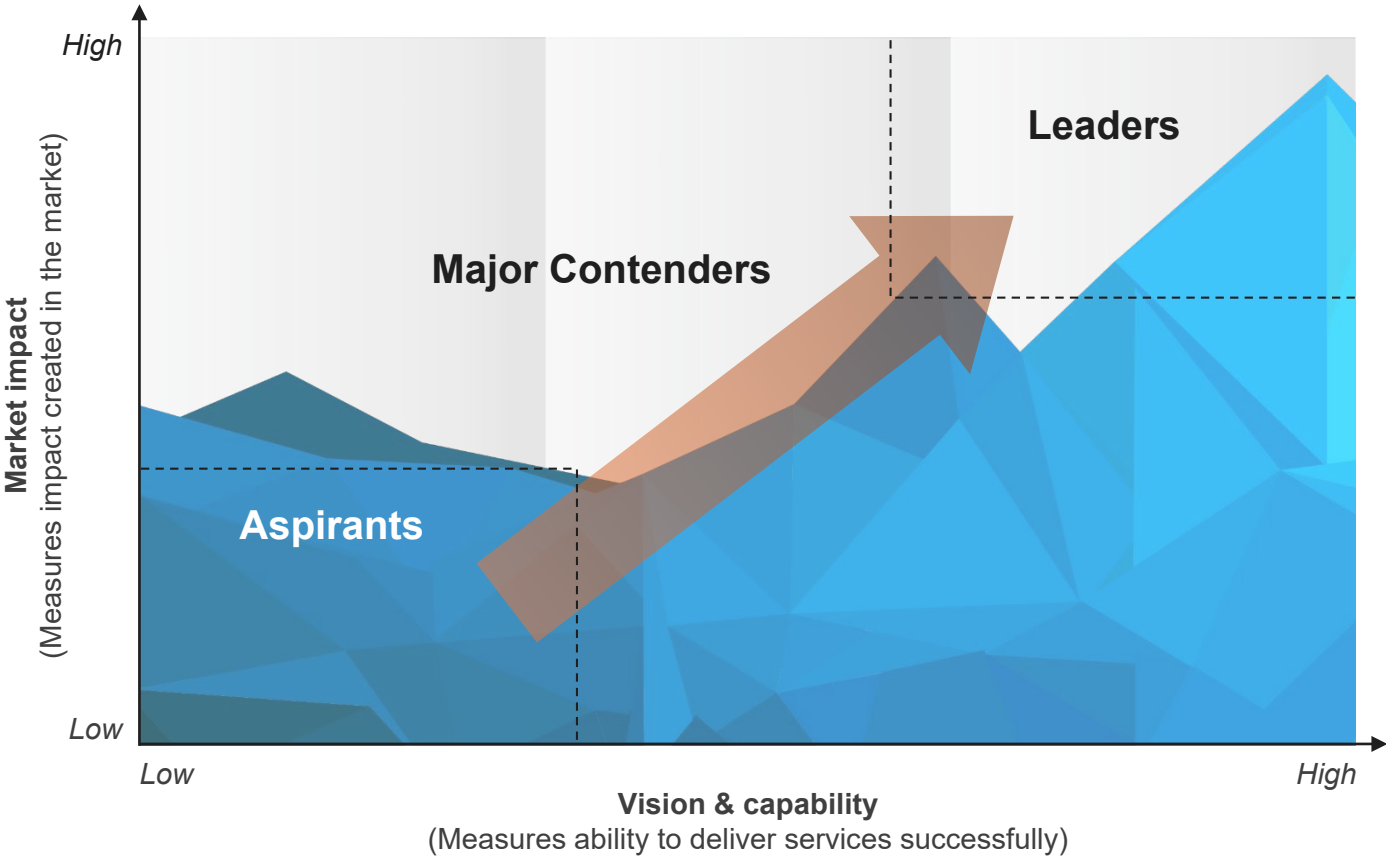
Investments (representative list)	
Investment name	Details
Acquisitions	Invested in seven acquisitions in 2021, to provide a full range of cybersecurity and operations across clients' IT and OT systems. Some of the acquisitions in the security area in North America include iDenfese, Fusion X, Cimation, Defense Point, Deja Vu Security, Revolutionary Security, and the US federal government services business of Endgame Inc..
Talent	<p>Accenture invested in talent in FY21 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: It has programs to nurture employees in cybersecurity and soft skills such as ecosystem of social learning, analytics, and certifications include CISSP, CIPP, SBASA, 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 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. Deepen industry, function, or technical knowledge and specialization—brings together material for over 14,000 colleagues and specialists• Online Master of Science in Cybersecurity (OMS Cybersecurity): This is offered in collaboration with Georgia Tech’s OMS Cybersecurity degree program to meet the demand for highly skilled cybersecurity professionals
Others	<ul style="list-style-type: none">• Cyber Security 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 Lab: The lab focuses on sensitive data discovery using machine learning, attack prediction via graph analytics, responsible AI, and application attack surface reduction

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

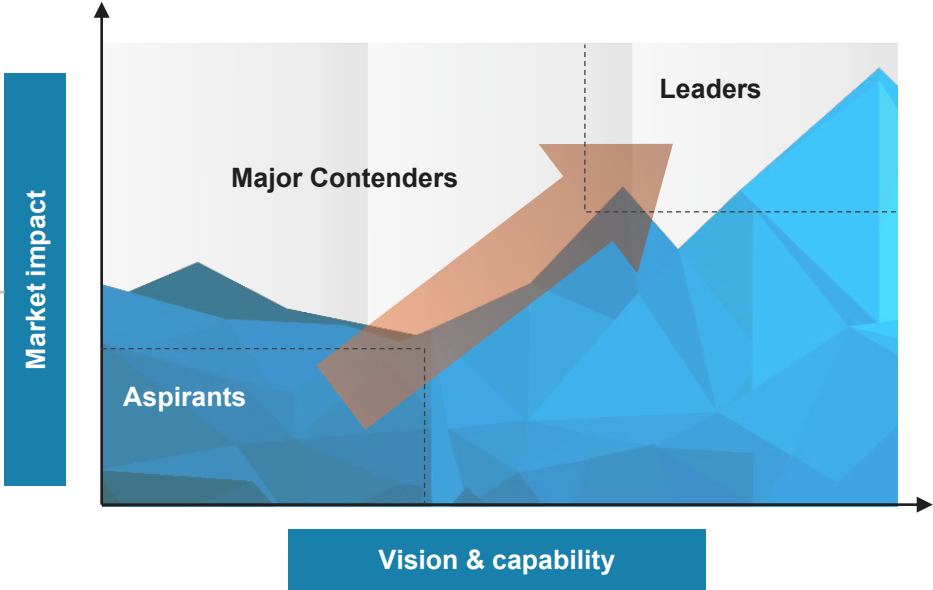
Number of clients, revenue base, YoY growth, and deal value/volume

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 adopts an unbiased and fact-based approach (leveraging provider / technology vendor RFIs and Everest Group's proprietary databases containing providers' deals and operational capability information). In addition, these results are validated / fine-tuned 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 PEAK Matrix assessment are relevant to buyers and providers besides the “PEAK Matrix position”?

A PEAK Matrix position is only one aspect of Everest Group's overall assessment. In addition to assigning a “Leader”, “Major Contender,” or “Aspirant” title, Everest Group highlights the distinctive capabilities and unique attributes of all the PEAK Matrix providers assessed in its report. The detailed metric-level assessment and associated commentary is helpful for buyers in selecting particular providers/vendors for their specific requirements. It also helps providers/vendors showcase their strengths in specific areas

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

- Participation incentives for buyers include a summary of key findings from the PEAK Matrix assessment
- Participation incentives for providers/vendors include adequate representation and recognition of their capabilities/success in the market place, and a copy of their own “profile” that is published by Everest Group as part of the “compendium of PEAK Matrix providers” profiles

What is the process for a provider / technology vendor to leverage their PEAK Matrix positioning and/or “Star Performer” status ?

- Providers/vendors can use their PEAK Matrix positioning or “Star Performer” rating in multiple ways including:
 - Issue a press release declaring their positioning. See [citation policies](#)
 - Customized PEAK Matrix profile for circulation (with clients, prospects, etc.)
 - Quotes from Everest Group analysts could be disseminated to the media
 - Leverage PEAK Matrix 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 the designated POC at Everest Group.

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

PEAK Matrix assessments are designed to serve present and future needs of the enterprises. 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 as well as serve the future expectations of enterprises



Everest Group is a research firm focused on strategic IT, business services, engineering services, and sourcing. Our research also covers the technologies that power those processes and functions and the related talent trends and strategies. Our clients include leading global companies, service and technology providers, and investors. Clients use our services to guide their journeys to maximize operational and financial performance, transform experiences, and realize high-impact business outcomes. Details and in-depth content are available 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.