Everest Group®

# Everest Group Cloud Security Services PEAK Matrix® Assessment 2025

Focus on TCS

February 2026

PEAK MATRIX®

# Introduction

As enterprises accelerate cloud adoption to enable digital agility, hybrid work, and AI-driven innovation, their cloud environments are becoming increasingly distributed and complex. This expanded ecosystem, spanning multi-cloud, edge, and Software-as-a-Service (SaaS) workloads, has increased the number of entry points for threats, driving the demand for unified visibility, continuous posture management, and zero-trust enforcement across layers.

Solutions such as Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), and broader Cloud-Native Application Protection Platform (CNAPP) capabilities have become integral to helping enterprises address misconfigurations, entitlement sprawl, and cross-cloud risks. In parallel, Cloud Workload Protection Platform (CWPP) capabilities are increasingly critical to securing virtual machines, containers, and serverless environments. Cloud security has thus evolved from a compliance function to a business enabler that underpins modernization, resilience, and innovation. Service providers are responding by embedding advanced automation, AI-driven threat detection, and contextual risk analytics into their offerings to help enterprises proactively mitigate misconfigurations, identity abuse, and cross-cloud data exposure.

Leading providers are building integrated delivery models that converge cloud, security, and DevSecOps capabilities, supported by platform investments, ecosystem partnerships, and Managed Detection and Response (MDR) capabilities tailored for cloud-native environments. As part of strengthening their SOC and MDR portfolios, many providers are also investing in Continuous Threat Detection and Response (CTDR) capabilities to enhance real-time monitoring and response across hybrid environments. In parallel, the demand for verticalized solutions, sovereign cloud controls, and secure-by-design migration frameworks is reshaping provider portfolios.

**The full report includes the profiles of the following 18 leading cloud security providers featured on the** Cloud Security Services PEAK Matrix® Assessment 2025:

- **Leaders:** Accenture, Deloitte, HCLTech, TCS, and Wipro
- **Major Contenders:** Capgemini, Cognizant, DXC Technology, IBM, Inspira Enterprise, Kyndryl, LTIMindtree, Mphasis, NTT DATA, and Persistent Systems
- **Aspirants:** Happiest Minds, YASH Technologies, and Zensar

## Scope of this report

**Geography:** global

**Industry:** all-encompassing industries globally

**Services:** cloud security

**Use cases:** cloud security use cases across foundational cloud security, cloud Identity and Access Management (IAM), cloud data security, cloud governance and compliance, and cloud application and runtime environment security

# Scope of the evaluation

This report examines provider capabilities and trends shaping the rapidly evolving cloud security services market

## Focus of research

### Consulting/assessment services

Cloud security strategy advisory, cloud security maturity assessment, zero-trust advisory, vulnerability assessment, policy and process consulting, security audits

### Design and implementation

Security architecture design, secure cloud migration and modernization, cloud-native security solution implementation, secure cloud configuration

### Managed services

Continuous threat detection, monitoring, reporting, and incident response, managed cloud security services, managed cloud governance, cloud visibility

**Cloud application and runtime environment security**

Secure application migration and modernization, application security testing, web application security including firewalls, cloud workload protection, DevSecOps services, SaaS applications security, app self protection, patching, operating system security, middleware security, container and microservices security, API security, cloud-native AI app security, AI runtime security, containerized AI deployment security

**Cloud IAM**

Authentication, authorization, access management, distributed identities, identity administration and management, multi-factor authentication, user provisioning, password management, PKI, privileged identity and access management, single sign on, agent identity security (including authentication, authorization, role enforcement for AI agents and autonomous workloads on cloud)

**Cloud data security**

Data encryption, certificate management, key management, Data Protection as-a-Service (DPaaS), tokenization, secure data migration and modernization, DLP services, database activity monitoring, data classification, data privacy and confidentiality solutions and services, protection of AI training data and models hosted in cloud

**Cloud governance and compliance**

Cloud security policy design and enforcement, risk management, governance framework adoption services, compliance, responsible AI use in cloud, cloud visibility, security standardization services across multi-cloud

**Cloud foundation security**

Landing zone security, cloud configuration management, cloud connect security, virtual private network security services, business continuity and disaster recovery services

Coverage across public cloud, private cloud, and multi-/hybrid cloud

# Cloud Security Services PEAK Matrix® characteristics

## Leaders

Accenture, Deloitte, HCLTech, TCS, and Wipro

- Leaders demonstrate a comprehensive cloud security portfolio spanning advisory, transformation, and managed security services, with strong capabilities in cloud-native security, zero-trust frameworks, and multi-cloud governance
- They are at the forefront of embedding AI and automation for continuous threat detection, compliance monitoring, and misconfiguration remediation, enabling proactive risk mitigation across complex hybrid environments
- Leaders exhibit deep platform partnerships with hyperscalers (AWS, Azure, and GCP), CSPM, and workload protection vendors, enabling integration-driven value creation
- They show strong delivery maturity, supported by extensive CoEs, global delivery presence, and industry-specific frameworks that align cloud security with business transformation goals

## Major Contenders

Capgemini, Cognizant, DXC Technology, IBM, Inspira Enterprise, Kyndryl, LTIMindtree, Mphasis, NTT DATA, and Persistent Systems

- Major Contenders bring strong capabilities in cloud infrastructure protection, workload security, and identity governance, often coupled with strong consulting and implementation expertise
- They are investing in automation utilities, migration accelerators, and compliance dashboards to strengthen efficiency and drive faster time-to-value in large-scale transformations
- Many are expanding their focus toward DevSecOps integration, data security, and AI-driven analytics while building proof points in areas such as agentic security orchestration and sovereign cloud enablement
- However, while these providers demonstrate consistency and scalability, their portfolio integration and their IP-led differentiation and innovation maturity remain relatively limited compared to Leaders, especially in delivering scalable and platform-enabled cloud security services

## Aspirants

Happiest Minds, YASH Technologies, and Zensar

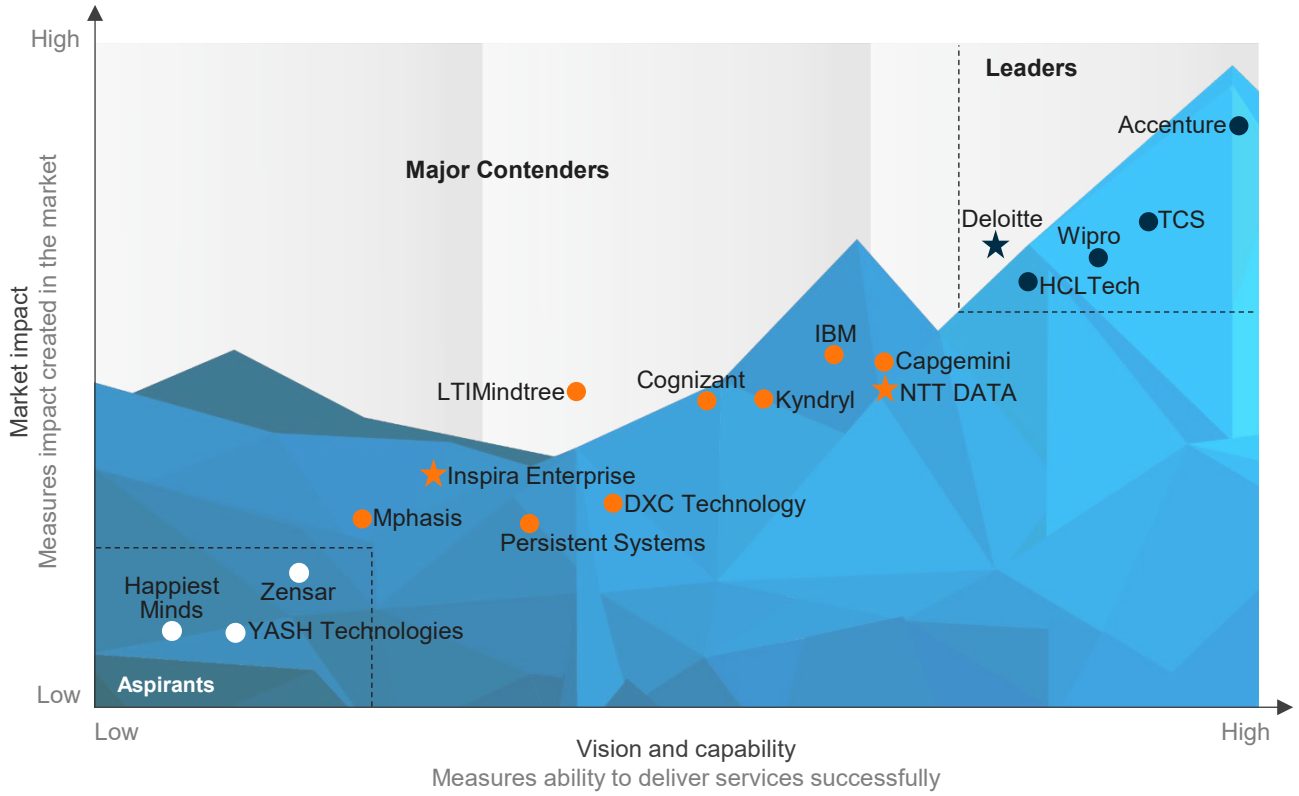
- Aspirants' differentiation lies in agility and client intimacy, offering competitive pricing, niche expertise, and flexible engagement models suited for mid-market and regional enterprises
- They are expanding through targeted partnerships, cloud-native MDR offerings, and managed compliance solutions, but generally lack the scale or global delivery footprint of larger peers
- Several are building early capabilities in AI-driven threat detection, cloud workload protection, and FinOps-integrated security management, often supported by IP-led utilities and accelerators
- Their challenge remains scaling delivery and demonstrating enterprise-grade maturity across multiple hyperscaler ecosystems and industry verticals

# Everest Group PEAK Matrix®

## Cloud Security PEAK Matrix® Assessment 2025 | TCS is positioned as a Leader

**Everest Group Cloud Security PEAK Matrix® Assessment 2025[1]**

- Leaders
- Major Contenders
- Aspirants
- ☆ Star Performers




1 Assessments for Capgemini, Deloitte, IBM, Happiest Minds, and Zensar 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 insurance buyers
Source: Everest Group (2025)

# TCS

## 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 comprehensive cloud protection and resilience can leverage TCS CNAPP and Cloud Shield.AI, embedding gen AI and automation to strengthen posture management, threat detection, and remediation across multi-cloud environments
- Enterprises seeking secure sovereign cloud capabilities can leverage TCS Sovereign Secure Cloud, which embeds zero-trust principles and sovereignty controls across hyperscaler landscape
- Enterprises seeking global and scalable cloud security delivery will find TCS's extensive network of delivery centers and geo-aligned CoEs beneficial for ensuring consistent and compliant support across regions
- Enterprises modernizing cloud security landscape can leverage TCS's Tech Debt Management framework to streamline tools, reduce redundancy, and enhance automation efficiency
- Some clients have appreciated TCS's responsiveness and account management approach, acknowledging its proactive engagement and flexibility in addressing ongoing cloud security needs

### Limitations

- Enterprises seeking mature partnerships across emerging and neo-cloud security ecosystems may find TCS's alliances in this area still at an early stage of maturity compared to peers
- Enterprises in retail, telecom, media and entertainment, and public sector verticals should be mindful of TCS's limited contextual expertise and engagement focus in these industries
- Some clients have expressed challenges with regards to the limited flexibility of commercial constructs and slower onboarding process while engaging with TCS
- Small and midsize enterprises should perform careful diligence before engaging with TCS due to its high focus on large-scale engagements
- Some enterprises have highlighted attrition as a major challenge for TCS due to limited knowledge transfer, impacting delivery quality

# Market trends

As cloud security adoption accelerates, enterprises are prioritizing cloud security posture management (CSPM), unified visibility, and AI-enabled protection while addressing multi-cloud complexity, data proliferation, and skill shortages amid rising AI and compliance risks

### Market size and growth

- Cloud security services represent a US$27-29 billion market in 2024, growing at 14-15% annually, driven by a need for securing expanding attack surfaces from multi-cloud adoption, cloud security posture management (CSPM), and the need to safeguard AI models and data pipelines
- Cloud foundation security accounts for the largest share of spend, followed by cloud identity and access management (IAM), as enterprises strengthen configuration, access, and identity governance
- North America leads adoption, while Europe and Asia Pacific are experiencing rapid growth fueled by digital transformation and regulatory modernization
- BFSI, public sector, and energy and utilities account for the largest share of cloud security spending, led by zero-trust adoption, digital sovereignty needs, and operational-technology convergence

## Key drivers for cloud security services

| | |
|---|---|
| Platform-led CNAPP consolidation | Enterprises seek integrated CNAPP ecosystems that unify CSPM, CIEM, CWPP, and CTDR to deliver full-stack visibility, automated remediation, and simplified governance across multi-cloud estates. |
| AI and gen AI-led security operations | Enterprises expect AI- and gen AI-enabled workflows for the cloud that enhance threat detection, response, and compliance efficiency while improving speed, accuracy, and resilience. |
| Cloud-native security | Enterprises require cloud-native security to ensure the protection of containerized workloads and microservices by enabling continuous validation, runtime defense, and secure DevSecOps integration across cloud-native environments. |
| Expanding threat landscape and secure cloud transformation | The rise in cloud-native attacks, identity misuse, misconfigurations, and supply chain vulnerabilities is driving enterprises to embed security-by-design into migration and modernization programs. |

## Opportunities and challenges for cloud security services

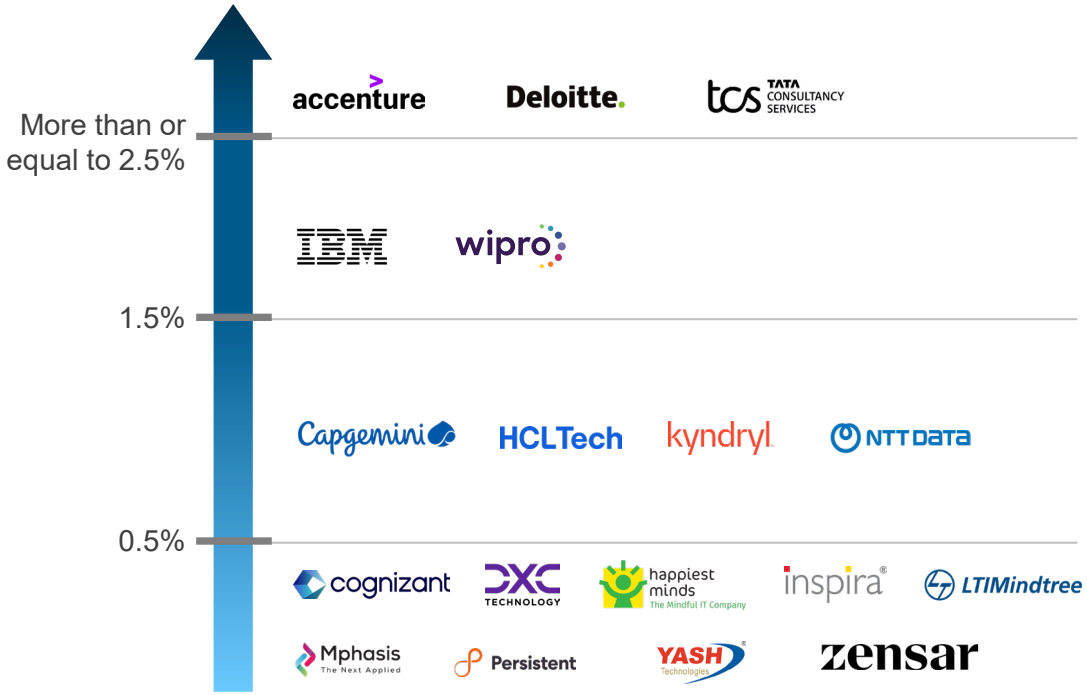
| | |
|---|---|
| AI governance and model risk | Enterprises face growing exposure from gen AI models and data pipelines moving across clouds, prompting stronger governance, data-integrity controls, and secure-by-design assurance frameworks. |
| multi-cloud complexity and fragmented controls | Enterprises struggle with inconsistent policies and tool sprawl across cloud environments, creating opportunities to adopt unified control planes and cross-platform governance for better visibility and compliance. |
| Investment and co-innovation imperatives | Rapid technology evolution and threat complexities are challenging enterprise agility, driving greater collaboration with hyperscalers and start-ups to develop integrated, adaptive security architectures. |
| Data proliferation and shared-responsibility gaps | The growing volume of sensitive data across hybrid and SaaS ecosystems is blurring accountability lines, pushing enterprises to strengthen data-centric security and shared-responsibility. |

# Provider landscape analysis

Market share and growth trends of cloud security service providers, showing competitive positioning and YoY performance

**Market share analysis of the providers[1]**

2024; percentage of the overall market of US$27-29 billion




**Provider market share by YoY growth[1]**

2024; increase in the percentage of revenue


1 Providers are listed alphabetically within each range

# Key buyer considerations

Enterprises are seeking partners that deliver end-to-end cloud security transformation, unified visibility, and AI-driven operations to achieve measurable outcomes and improved cloud security posture

## Key sourcing criteria

High

Priority

Low

### End-to-end cloud security transformation

Buyers prefer partners that can design, modernize, and manage cloud security programs holistically, demonstrating measurable posture improvement through automation-first delivery models.

### Unified CNAPP and zero-trust integration

Buyers seek partners offering integrated CSPM, CIEM, CWPP, and CTDR capabilities that deliver cross-cloud visibility, policy consistency, and zero-trust alignment across multi-cloud environments.

### AI-driven operations and responsible governance

Buyers favor providers embedding gen AI and automation into security operations center (SOC) and compliance workflows, while ensuring responsible AI use through explainable governance and AI TRiSM controls.

### Evolving deal constructs

Buyers are favoring modular, outcome-linked contracts that emphasize measurable posture gains, faster remediation, and transparent governance within co-managed delivery models.

### IP-led innovation and ecosystem leverage

Buyers value partners bringing proprietary accelerators, reusable infrastructure-as-code (IaC) libraries, and hyperscaler and independent software vendor (ISV) co-innovation programs that enhance speed, scalability, and modernization efficiency.

## Summary analysis

Enterprises are redefining sourcing priorities as end-to-end cloud security transformation, CNAPP integration, and AI-enabled operations reshape expectations from cloud security partners.

Buyers now emphasize measurable outcomes through unified visibility, shared accountability, and modular deal frameworks that balance agility with control.

At the same time, IP reuse and ecosystem-led innovation remain key to achieving scalable, efficient, and future-ready delivery.

# Key takeaways for buyers

Cloud security buyers should prioritize providers that offer automation-led cloud security transformation, cross-cloud visibility, and AI-enabled protection to strengthen risk management and compliance across hybrid environments. Providers with strong innovation ecosystems, reusable IP, and scalable delivery models will be best positioned to deliver secure, efficient, and future-ready cloud security outcomes.

## AI-led security transformation

AI-enabled SOC and compliance automation are driving speed, accuracy, and accountability while securing AI and gen AI models through explainable and responsible AI frameworks.

## Unified visibility and zero-trust enabled controls

Integrated CNAPP and zero-trust architectures that ensure cross-cloud governance, continuous compliance, and policy consistency are becoming baseline enterprise requirements.

## Innovation and ecosystem-led modernization

Proprietary accelerators, reusable IaC libraries, and co-engineering with hyperscalers and ISVs are helping buyers achieve faster deployments, cost efficiency, and modernization scale.

## Scalable and automation-led delivery model

Providers with certified talent pools, automation-led delivery models, and scalable Center of Excellence (CoE) structures are emerging as partners of choice for managing complexity and maintaining agility.

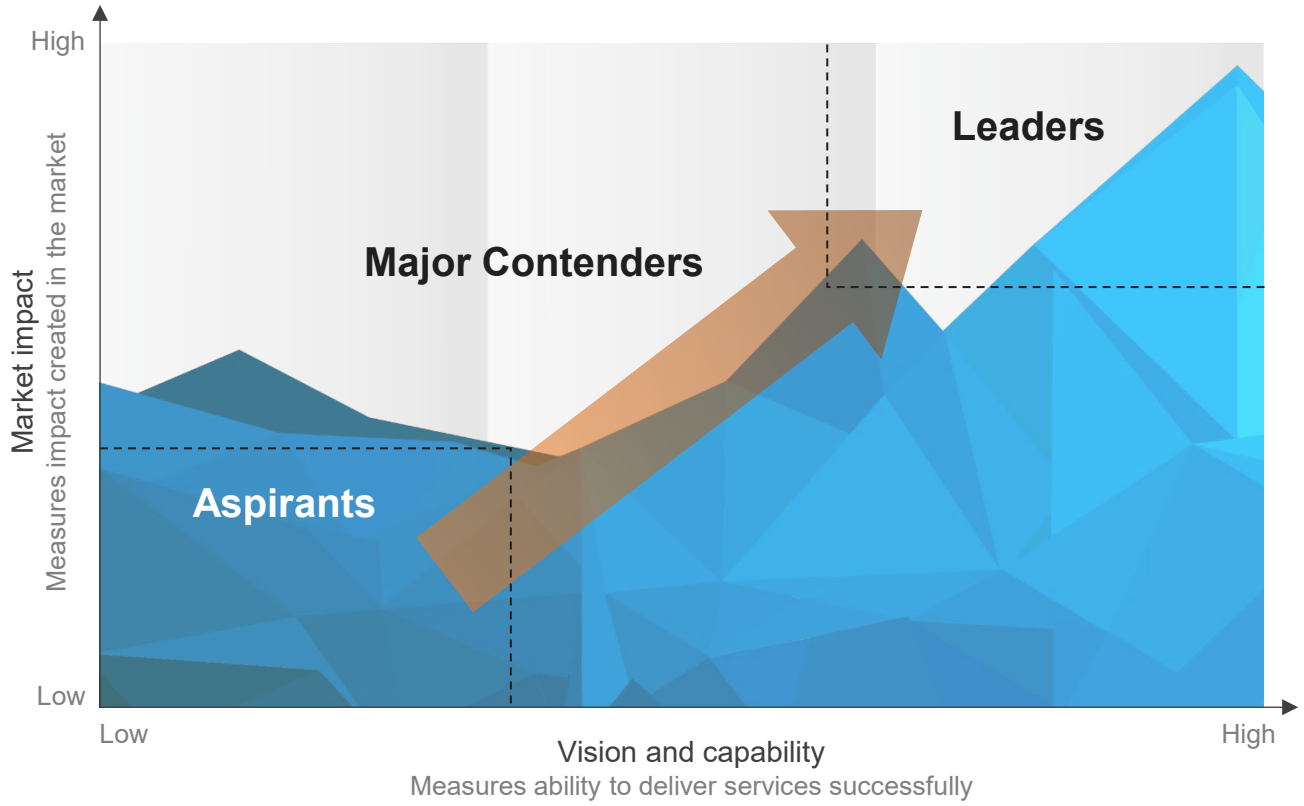
# Appendix

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**



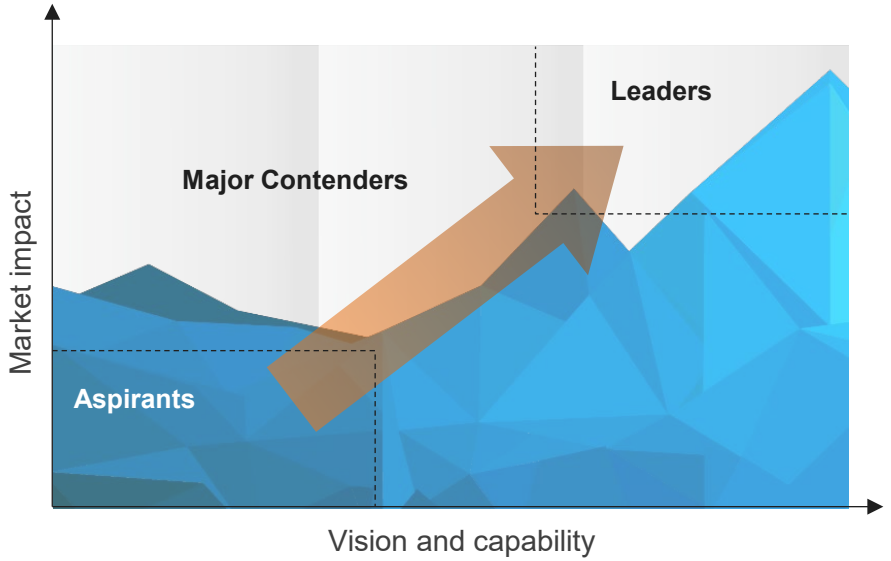
# Services PEAK Matrix® evaluation dimensions

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 organization 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**.



Everest Group®
With you on the journey