Everest Group®

Everest Group Cybersecurity Services PEAK Matrix® Assessment 2026 – Global

Focus on Accenture

August 2026

PEAK MATRIX®

Introduction

Cybersecurity has become a core business priority as enterprises expand their digital estates, adopt cloud and AI, and face more sophisticated threats. Buyers are increasing investments across advisory, implementation, and managed services to strengthen protection, improve resilience, and meet evolving regulatory requirements.

The market has also become more globally distributed. Demand is accelerating across Asia Pacific, the Middle East, and other emerging regions, alongside continued growth in North America and Europe. At the same time, delivery models are becoming more global, while data localization, sovereignty, and cross-border regulatory considerations are gaining importance.

This assessment tracks several themes shaping the next phase of cybersecurity services. These include AI security and enterprise AI risk governance, machine identity and non-human access management, and AI-augmented security operations. It also examines sovereign cloud, data localization, critical infrastructure protection, crypto-agility, and post-quantum readiness.

Cyber resilience is becoming equally important as enterprises prepare for operational disruption, geopolitical risk, and increasingly complex attack scenarios. Service providers are therefore expanding their focus from prevention and detection toward recovery, continuity, and measurable risk reduction.

The full report includes the profiles of the following 32 leading cybersecurity service providers featured on the Cybersecurity Services PEAK Matrix® Assessment 2026 – Global:

- **Leaders:** Accenture, Cognizant, Deloitte, EY, HCLTech, IBM, TCS, and Wipro
- **Major Contenders:** Atos, Capgemini, Computacenter, CyberProof, DXC, EPAM, FIS, Infosys, Inspira Enterprise, Kyndryl, LanceSoft, LTM, Mphasis, NTT DATA, Orange Cyberdefense, Persistent Systems, PwC, Tech Mahindra, and Zensar
- **Aspirants:** Birlasoft, Telefonica, TP Group, Unisys, and YASH Technologies

Scope of this report

Geography: global

Industry: all industries

Services: cybersecurity services

Use cases: 90+ distinct use cases

Scope of the evaluation

This report focuses on cybersecurity services and offers insights into the key cybersecurity services market trends

Consulting/assessment services

Cybersecurity strategy and roadmap development, security operating model and governance design, security architecture/modernization advisory, CISO/board-level cyber advisory, penetration testing, red/purple teaming, and adversary emulation

Design and implementation

Security architecture design, tool implementation and integration, platform migration and modernization, control configuration and tuning, and automation and orchestration enablement

Management and monitoring services

Managed security services for operating and maintaining security platforms and controls, including SOC operations, SIEM/MDR/SOAR/XDR platform management, and incident-response coordination and containment

Control plane

Identity and access management

Authorization, continuous and risk-based authentication, IGA, PAM, identity-driven access controls and policy enforcement, identity federation, SSO, MFA, password-less access, lifecycle management, access certification and reviews, and identity analytics and reporting

Cyber resilience and recovery

Automated point-in-time / granular recovery, disaster recovery orchestration, quick Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), data resiliency-as-a-service, disaster recovery-as-a-service, High Availability (HA), and failover and failback automation

Data security

Data discovery, classification, and tagging, data access governance and monitoring, DLP, encryption, tokenization and data masking, PQC readiness and migration planning, crypto-agility, and hybrid cryptography

Governance, Risk, and Compliance (GRC)

GRC management, GRC-as-a-service, risk assessment as-a-service, compliance audits, compliance assurance, third-party risk management, vulnerability and patch management, risk quantification, and security awareness training

Application and software supply chain security

Application security testing (SAST, DAST, IAST, SCA, etc.), secure coding and code reviews, pen-testing, API security, DevSecOps and CI/CD pipeline security, software supply chain security (SBOMs, provenance, artifact signing), and runtime application protection

Threat management

Endpoint Detection and Response (EDR), Host Intrusion Prevention Systems (HIPS), virus and malware protection, threat detection, hunting, and response across end points, cloud, applications, IoT, OT, network, etc., threat intelligence, monitoring and reporting, digital forensics, log analysis, reduced MTTD and MTTR, vulnerability scanning and prioritization, exposure management and ASM, breach and attack simulation, and threat intelligence enrichment

AI security

AI training data protection, model artifact, prompt, and output security, LLM red-teaming and adversarial testing, prompt injection and poisoning defenses, model access control and authentication, runtime attack detection, threat modeling for AI systems, secrets management for agents, and model integrity verification

Infrastructure plane

Network security

Firewalls, Next-generation Firewalls (NGFW), email / URL gateways, Network Intrusion Prevention Systems (NIPS), Distributed Denial-of-Service (DDoS) prevention and mitigation, Unified Threat Management (UTM), VPN, Advanced Persistent Threat (APT) solutions, network-access control, ZTNA, SSE, SASE, gateway security, edge security, edge runtime protection, and edge monitoring

IoT and OT security

IoT device and data protection, asset discovery and intelligence, IoT threat intelligence, communication channel security, pre-embedded IDs and encryption, API access control, firmware update on IoT devices, OT device security, and OT device monitoring

Cloud security

Cloud security architecture, landing zones, and guardrails, CSPM, CWPP, CNAPP, container and Kubernetes security, workload runtime security, cloud foundation security, and misconfiguration management

Characteristics of Leaders, Major Contenders, and Aspirants

Leaders

Accenture, Cognizant, Deloitte, EY, HCLTech, IBM, TCS, and Wipro

- Leaders combine broad consulting, implementation, and managed services with global delivery scale, deep industry coverage, and strong client traction across cybersecurity segments
- They are advancing AI-led operations, security for AI, cyber resilience, sovereignty, and PQC through proprietary platforms, accelerators, and mature technology ecosystems
- However, they must convert emerging capabilities into repeatable deployments and measurable outcomes while sustaining differentiation in a competitive market

Major Contenders

Atos, Capgemini, Computacenter, CyberProof, DXC, EPAM, FIS, Infosys, Inspira Enterprise, Kyndryl, LanceSoft, LTM, Mphasis, NTT DATA, Orange Cyberdefense, Persistent Systems, PwC, Tech Mahindra, and Zensar

- Major Contenders demonstrate credible capabilities in selected areas such as MDR, IAM, cloud security, OT security, cyber resilience, and regulatory transformation
- Many are investing in agentic SOC, security for AI, PQC, sovereignty, proprietary IP, and partner-led modernization, although adoption and proof points remain uneven
- To challenge Leaders, they need stronger global execution, broader managed services traction, deeper industry solutions, and clearer evidence of outcome-led delivery

Aspirants

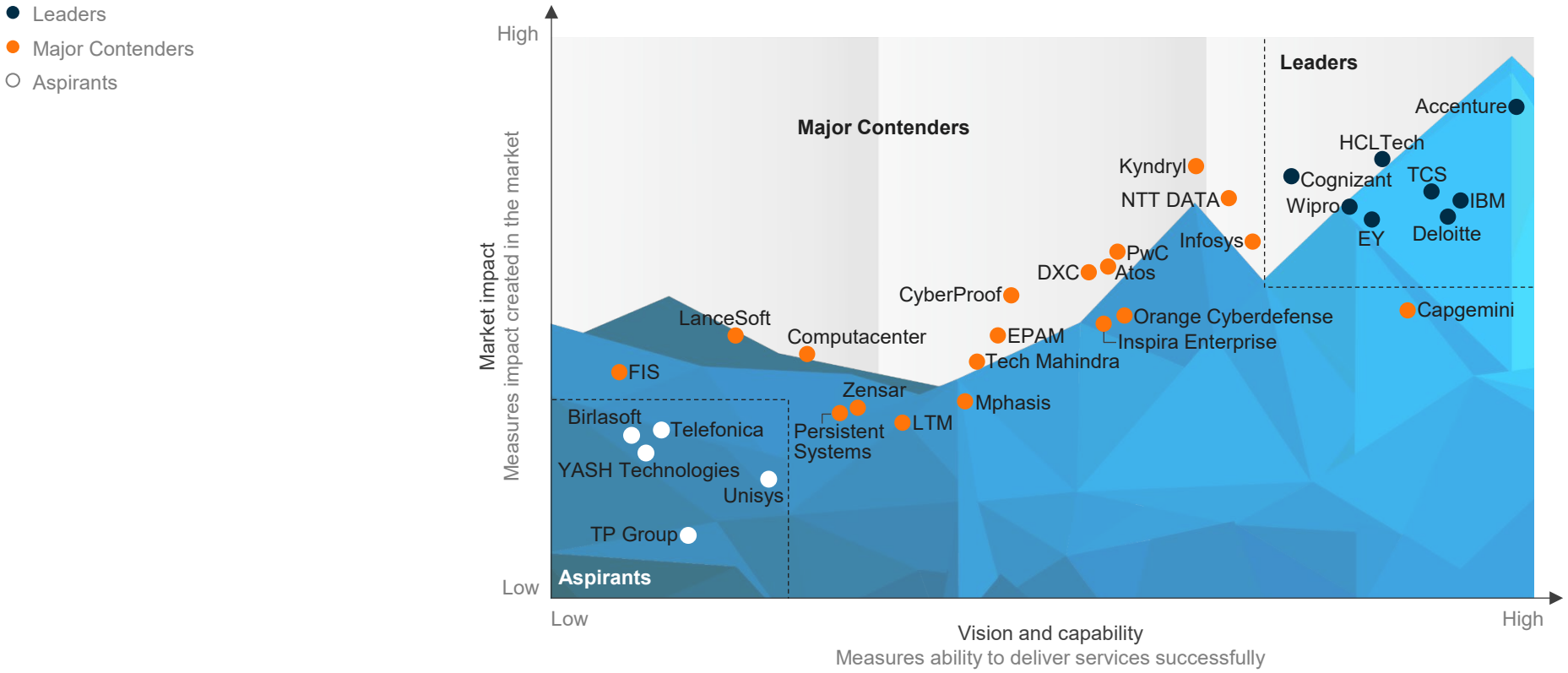
Birlasoft, Telefonica, TP Group, Unisys, and YASH Technologies

- Aspirants have selective cybersecurity capabilities, with narrower service coverage, smaller delivery footprints, and fewer large-enterprise proof points across regions and industries
- They are building AI-enabled SOC, cloud, identity, GRC, and resilience offerings through targeted IP, talent, and partnerships, but most next-generation capabilities remain early stage

Everest Group PEAK Matrix®

Cybersecurity Services PEAK Matrix® Assessment 2026 – Global | Accenture is positioned as a Leader

Everest Group Cybersecurity Services PEAK Matrix® Assessment 2026 – Global[1]



1 Assessments for Atos, Deloitte, PwC, Tech Mahindra, and Unisys exclude 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 (2026)

Accenture

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 an end-to-end cybersecurity partner can consider Accenture for its coverage across cybersecurity strategy, IAM, cloud, data, cyber defense, resilience, OT, and secure AI, delivered through consulting, design and implement, and managed services
- Enterprises seeking fast risk assessment and remediation can leverage Accenture's Cyber.AI platform, which unifies signals from existing security tools to identify, prioritize, and address cyber risks
- Accenture's partnerships across hyperscalers and leading cybersecurity technology providers can benefit enterprises undertaking ecosystem-led modernization
- Enterprises preparing for emerging risks can consider Accenture for its offerings across secure agentic AI, sovereign cybersecurity, and post-quantum readiness, spanning governance, identity, infrastructure, cryptographic discovery, and transformation roadmaps
- Enterprises requiring global cybersecurity delivery can benefit from Accenture's distributed security centers, SOC network, and structured cyber talent development programs

Limitations

- Enterprises seeking uniformly mature AI-led cybersecurity delivery should assess Accenture, as several Cyber.AI capabilities remain in early-client, pilot, or development stages
- Client feedback indicates that talent continuity can be inconsistent, with turnover, skill alignment, and retention of technical leads requiring attention
- Clients highlighted that Accenture's transformation-led delivery, proprietary IP, and multi-partner constructs can increase commercial complexity and overall engagement costs
- Client feedback indicates that the initial ramp-up required substantial enterprise-specific learning, making structured onboarding, knowledge transfer, and early domain-context validation important at engagement outset
- Clients indicate that Accenture's commercial models remain more weighted toward hybrid and fixed-price constructs than pure outcome-linked pricing

Market trends

Enterprises are accelerating cybersecurity services adoption to strengthen resilience, secure AI-led transformation, modernize fragmented estates, and address persistent talent gaps

Market size and growth

- The global cybersecurity services market is estimated at US$110-115 billion, supported by expanding attack surfaces, regulatory scrutiny, cloud adoption, and increasing enterprise dependence on digital operations
- Managed security services account for a growing share of demand as enterprises seek continuous monitoring, specialist expertise, and scalable security operations amid persistent talent constraints
- North America remains the largest market, while Europe is experiencing strong demand from regulatory requirements, cyber sovereignty priorities, and regional delivery considerations

Key drivers for cybersecurity services

Security for AI	Gen AI applications and autonomous agents are creating demand for AI governance, model and data protection, agent identity, runtime monitoring, and protection against emerging AI-specific threats.
Cyber resilience and regulatory readiness	Boards are placing greater emphasis on recovery, business continuity, incident preparedness, and measurable cyber-risk reduction as regulatory and disclosure requirements expand.
Cybersecurity modernization	Enterprises are modernizing fragmented security estates across cloud, identity, applications, data, and infrastructure to improve visibility, scalability, and cost efficiency.

Opportunities and challenges

Legacy and fragmented security estates	Disparate tools, inherited infrastructure, and siloed operating models restrict visibility, creating opportunities for platform consolidation, SIEM modernization, and phased transformation.
Growth of non-human identities	AI agents, APIs, workloads, and service accounts require stronger identity discovery, least-privilege access, secrets management, and continuous governance.
Safe adoption of agentic security	Concerns around autonomy, accountability, and erroneous actions increase demand for guardrails, human approvals, rollback controls, and auditability.
Talent and delivery constraints	Shortages in AI, cloud, OT, identity, and threat-management skills are increasing reliance on managed services, automation, specialized CoEs, and global delivery models.

Provider landscape analysis

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

Market share analysis of the providers[1]

2025; percentage of the overall US$110-115 billion market

Provider market share by YoY growth[1]

2024-25; overall market growth of 14-16%

1 Providers are listed alphabetically within each range

Key buyer considerations

Buyers prioritize transformation depth, AI-enabled operations, domain expertise, measurable outcomes, and the ability to operate complex security estates at scale

Key sourcing criteria

High

Priority

Low

Cyber transformation and operating model expertise

Buyers seek providers that can redesign security architecture, processes, and operating models while supporting implementation and ongoing operations.

AI-enabled security operations with governance

Enterprises assess the provider's ability to apply AI across detection, investigation, response, and vulnerability management with strong controls and human oversight.

Industry-aligned risk and regulatory expertise

Buyers value providers that understand sector-specific threats, regulatory obligations, cyber resilience requirements, and regional data and sovereignty considerations.

Ability to modernize fragmented security estates

Providers are expected to consolidate tools, integrate security platforms, and improve visibility across cloud, identity, data, applications, infrastructure, and OT environments.

Measurable outcomes and commercial flexibility

Provider selection increasingly depends on demonstrable risk reduction, productivity improvement, service-level accountability, and outcome-linked models.

Summary analysis

Cybersecurity sourcing decisions are increasingly shaped by the provider's ability to combine strategic transformation with scalable, technology-enabled operations.

Buyers are placing greater emphasis on AI-led productivity, but expect clear governance, explainability, human intervention, and integration with existing security workflows.

Industry expertise and regulatory alignment remain critical, particularly across highly regulated and sovereignty-sensitive sectors.

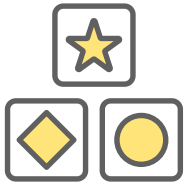
The ability to simplify fragmented security estates is becoming a major differentiator as enterprises seek improved visibility, lower operating complexity, and better value from existing investments.

Key takeaways for buyers

Cybersecurity sourcing is moving beyond service breadth, with buyers prioritizing transformation depth, AI-enabled delivery, industry relevance, and measurable risk reduction.

AI-led operations with controlled autonomy

Providers are applying AI across detection, investigation, response, vulnerability management, and compliance, making governance, human oversight, and workflow integration critical buying considerations



Consolidation and resilience are converging

Enterprises want to simplify fragmented security estates while improving recovery and continuity, creating demand for providers that can modernize without disrupting operations

Industry and outcome alignment matter more

Sector expertise, regulatory readiness, regional delivery, and flexible pricing are becoming stronger differentiators, with sourcing decisions increasingly linked to measurable security and resilience outcomes

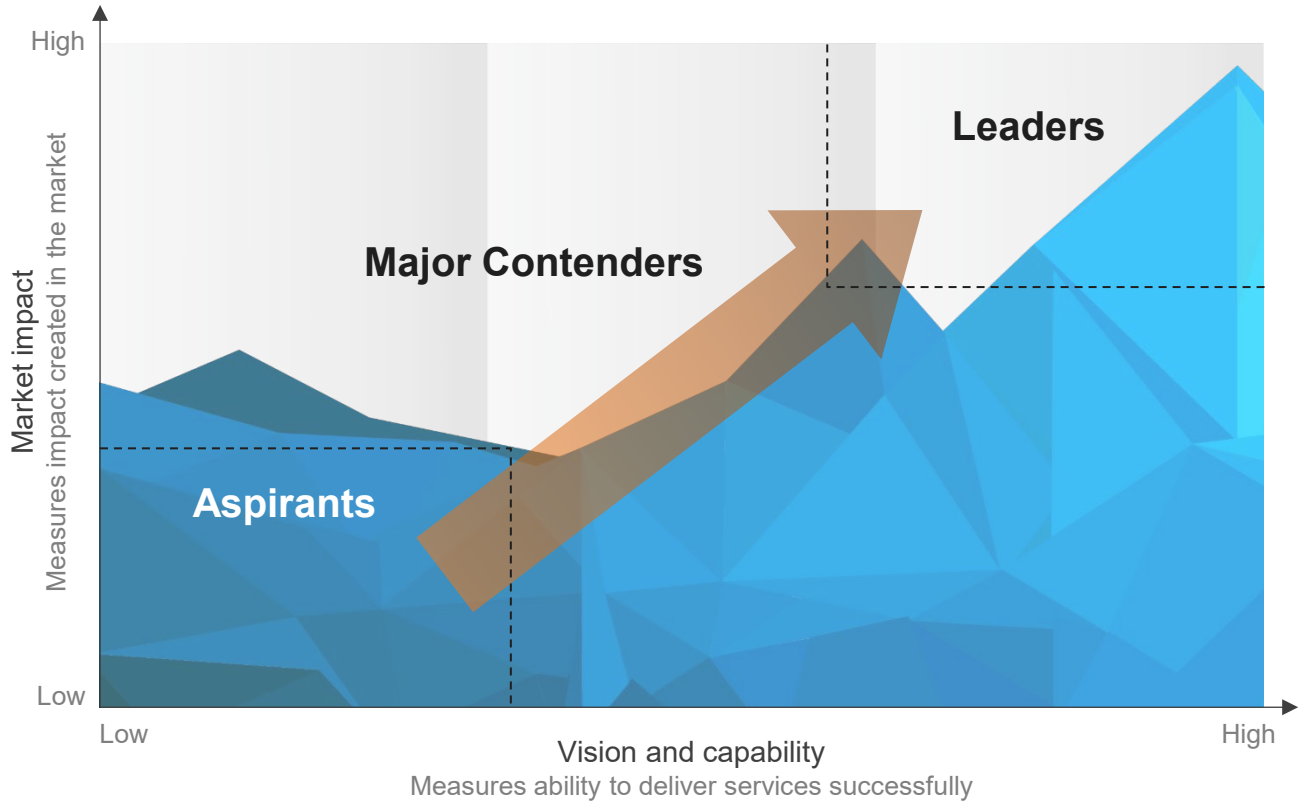
Appendix

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



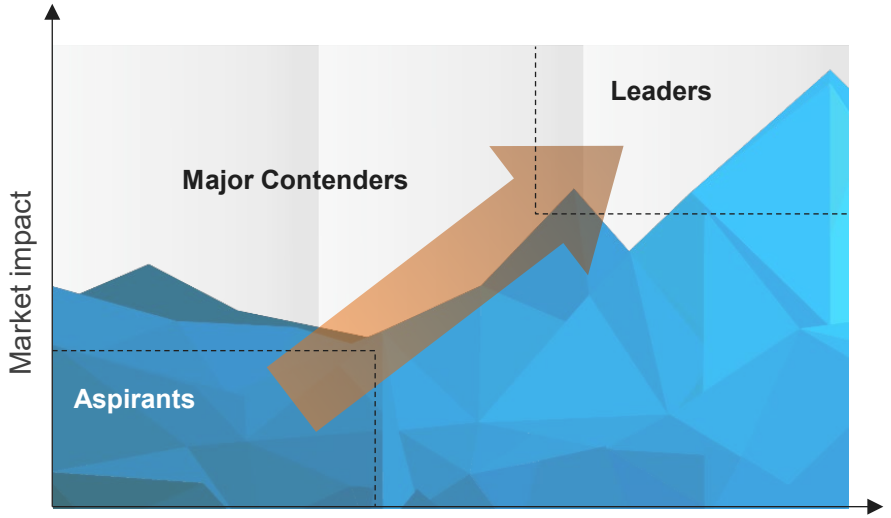
Services PEAK Matrix® evaluation dimensions

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