



Everest Group Cybersecurity Services PEAK Matrix® Assessment 2024 – North America

Focus on Wipro

October 2024



Introduction

The increasing reliance on digital technologies in North America has driven a significant rise in the demand for robust cybersecurity services. The rapid adoption of cloud computing, IoT devices, and remote work has expanded the attack surface for cybercriminals, making organizations more vulnerable to sophisticated threats such as data breaches and ransomware. This has created urgent challenges for enterprises including complex cyber threats, a shortage of skilled professionals, and strict regulatory requirements.

Service providers are developing advanced cybersecurity solutions such as AI-driven threat detection, zero trust, Secure Access Service Edge (SASE), gen AI security, quantum security, and autonomous Security Operations Center (SOC) to cater to these challenges. They are also investing in talent development and automation to address the skills gap. As the digital landscape evolves, the focus on proactive and adaptive security measures is expected to drive continued growth in cybersecurity.

In this research, we present an assessment and detailed profiles of 30 cybersecurity service providers from the North

American region, featured on the [Cybersecurity Services PEAK Matrix® Assessment 2024 – North America](#). The assessment is based on Everest Group's annual RFI process for the calendar year 2024, interactions with leading cybersecurity service providers, client reference checks, and ongoing analysis of the cybersecurity services market.

The full report includes the profiles of the following 30 leading cybersecurity service providers featured on the **Cybersecurity Services PEAK Matrix® Assessment PEAK Matrix 2024 – North America**:

- **Leaders:** Accenture, Deloitte, EY, IBM, Kyndryl, HCLTech, TCS, and Wipro
- **Major Contenders:** AT&T, CGI Group, Cognizant, DXC Technology, EPAM, Eviden, Fujitsu, GuidePoint Security, Happiest Mind, Infosys, LTIMindtree, NTT DATA, Tech Mahindra, CyberProof, Verizon, PwC, and WWT
- **Aspirants:** Aujas, Harman, Innova Solutions, Orion Innovation, and Yash Technologies

Scope of this report

Geography: North America

Industry: All-encompassing industries globally

Services: Cybersecurity services

Use cases: Only publicly available information (~90 distinct use cases) has been used for the entire analysis in this report

Cybersecurity services PEAK Matrix® characteristics

Leaders

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

- Leaders in cybersecurity aim to stay at the forefront of key cybersecurity segments such as Identity and Access Management (IAM), cloud security, Managed Detection and Response (MDR), Operational Technology (OT) security, and application security by delivering comprehensive, end-to-end cybersecurity solutions that build trust and confidence among enterprises, ensuring they are well-prepared to tackle emerging threats
- Leaders demonstrate exceptional proactiveness by driving innovations and introducing next-generation cybersecurity solutions including SASE, quantum security, gen AI security, and decentralized identity, among others
- Leaders offer co-innovative cybersecurity solutions, driven by a strong partnership ecosystem with leading technology providers

Major Contenders

AT&T, CGI Group, Cognizant, CyberProof, DXC Technology, EPAM, Eviden, Fujitsu, GuidePoint Security, Happiest Mind, Infosys, LTIMindtree, NTT DATA, Tech Mahindra, Verizon, PwC, and WWT

- Major Contenders present formidable competition to market leaders, making a significant impact with consistent YoY growth and delivering sustainable value to their cybersecurity clients
- These participants consistently invest in building IP, accelerators, and point solutions, while expanding services to address gaps. However, their portfolios are not as comprehensive as those of industry leaders, which is evident in their more limited market impact
- These players have partnerships with major cybersecurity technology vendors for joint Go-to-market (GTM) and training initiatives

Aspirants

Aujas, Harman, Innova Solutions, Orion Innovation, and Yash Technologies

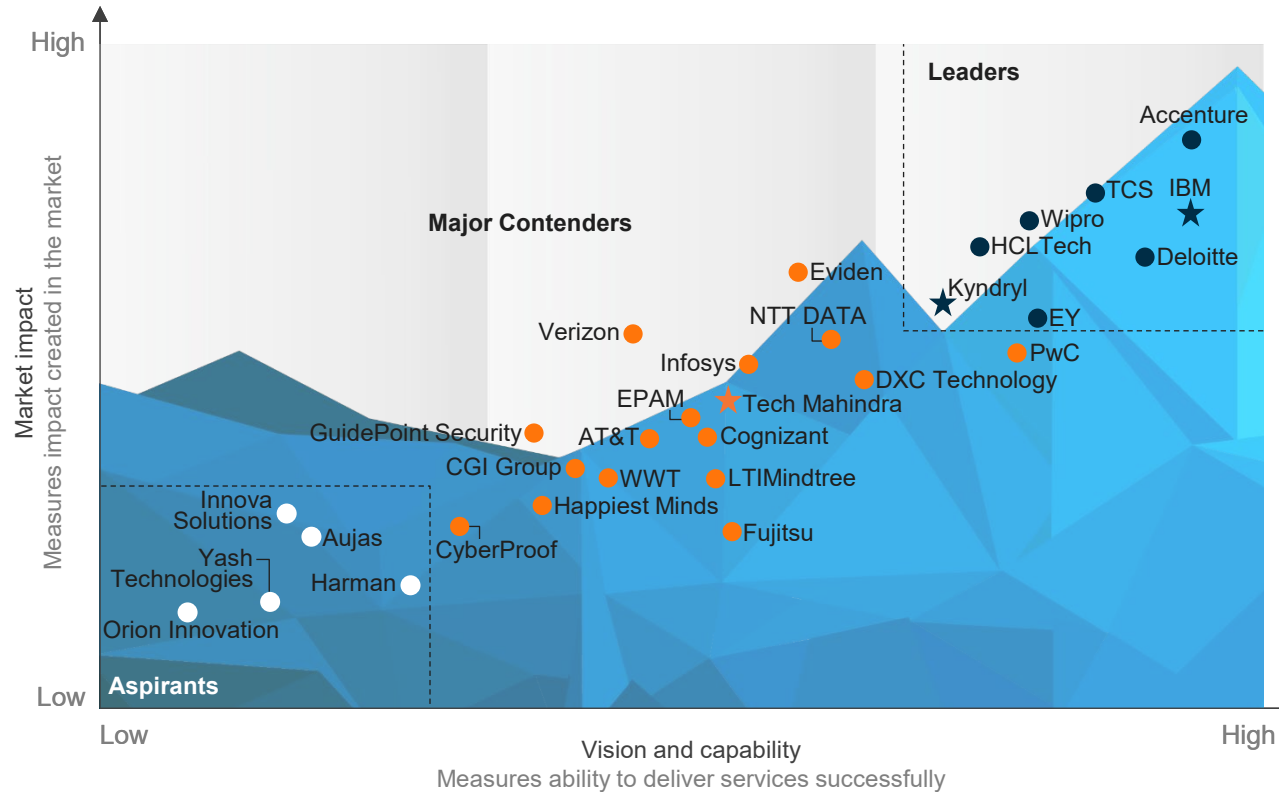
- The cybersecurity business of the Aspirants is still in its early stages and does not cater to large or mega clients in the domain. These providers specialize in limited segments of cybersecurity, offering a narrow scope of services
- These providers are actively broadening their cybersecurity capabilities by leveraging strategic services, enhancing skills, and developing IP-driven solutions to better serve their clients

Everest Group PEAK Matrix®

Cybersecurity Services PEAK Matrix® Assessment 2024 – North America | Wipro is positioned as a Leader

Everest Group Cybersecurity Services PEAK Matrix® Assessment 2024 – North America¹

- Leaders
- Major Contenders
- Aspirants
- ☆ Star Performers



¹ Assessments for AT&T, CGI Group, Deloitte, PwC, and WWT excludes service provider inputs and are based on Everest Group's proprietary Transaction Intelligence (TI) database, provider public disclosures, and Everest Group's interactions with buyers
Source: Everest Group (2024)

Wipro provider profile – North America (page 1 of 7)

Overview

Vision

Wipro helps businesses around the world achieve a resilient cyber future. It aspires to assist enterprises in building a cybersecurity posture that complements business growth. Wipro is exploring evolving industries and technologies in cybersecurity to stay at the forefront of technological advances and be a purposeful contributor to the cyber community. It aims to be the long-term partner of enterprises in their cybersecurity implementation journey.

Cybersecurity services revenue – North America (CY 2024)

<US\$200 million	US\$200-500 million	US\$500 million-1 billion	>US\$1 billion
------------------	----------------------------	---------------------------	----------------

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

Adoption by industry

- BFSI
- Energy and utilities
- Manufacturing
- Electronics, hi-tech, and technology
- Healthcare and life sciences
- Telecom, media, and entertainment
- Public sector
- Retail and CPG

Adoption by service segments

- Application security
- Cloud security
- Data security
- Identity and access management
- IoT and OT security
- Risk, vulnerability management and compliance
- Disaster recovery
- End-point security
- Network security
- Threat management

Adoption by buyer group

- Small (annual client revenue <US\$1 billion)
- Midsize (annual client revenue US\$1-5 billion)
- Large (annual client revenue >US\$5 billion)

Adoption by geography

- US
- Canada
- Mexico

Source: Everest Group (2024)

Wipro provider profile – North America (page 2 of 7)

Case studies

[NOT EXHAUSTIVE]

CASE STUDY 1

Accelerated application onboarding to SailPoint for a US-based financial corporation

Business challenge

The client faced significant challenges with its application migration and onboarding process. The transition from SunIDM to SailPoint was severely delayed, and tight deadlines required the migration of nearly 200 applications within a year. Frequent changes in requirements led to unnecessary rework, and manual provisioning and de-provisioning for disconnected applications contributed to operational inefficiencies. These inefficiencies resulted in high costs, resource demands, errors, and a large volume of support tickets related to User Access Management (UAM). Additionally, the lack of automation and improvements in certification, QA, and reconciliation processes further exacerbated these issues.

Solution

To streamline the information gathering process and reduce the burden on application teams, Wipro enhanced the AppOn tool. It extracted existing application data from SunIDM and presented it to application teams for validation through a custom-built User Interface (UI). The UI also automated the collection of additional information. This accelerated the onboarding of approximately 400 applications to SailPoint using Wipro's AppOn accelerator within a year. An average of 15, and at most 30, applications were onboarded per release cycle. Additionally, Wipro automated UAM for around 300 disconnected applications using a Selenium-/AutoIT-based framework within a year.

Impact

- 400 applications onboarded to SailPoint within 12 months, using Wipro accelerators
- UAM automation for 300 applications, thus leading to cost savings for customer
- Reduction in 80% of UAM ticket handling efforts achieved through automation
- Improved SLAs for manual UAM tasks and operational efficiency through streamlined processes
- Automation of routine QA and reconciliation tasks

CASE STUDY 2

Offered strategic installation and managed services support for Azure Cloud security for a US-based healthcare organization

Business challenge

The client was searching for a partner that could provide end-to-end security in design, architecture, implementation, and compliances, as well as improve the security posture to help it fulfill regulatory obligations.

Solution

The scope included migration of legacy antivirus tools to Microsoft Defender for antivirus with implementation and configuration of defender for end point, migration of workload from on-premise to Azure Cloud, and managed security support services for Endpoint Detection and Response (EDR), security monitoring, and data security and 24*7 cloud security support for using on-call support with a common L1 monitoring team.

Impact

- Added 120 new cloud workloads for scanning that were not previously scanned by the incumbent, resulting in the discovery of thousands of new vulnerabilities
- Reduced FTE count by 40% across the monitoring tracks with the cross-skilling of Security Operations Center (SOC) monitoring personnel across applications, infrastructure, and security
- Initiated continuous improvement activities such as Single Sign-on (SSO) and Multi-factor Authentication (MFA) for all internal and external users, as well as a data loss prevention program for important applications

Source: Everest Group (2024)

Wipro provider profile – North America (page 3 of 7)

Solutions

[NOT EXHAUSTIVE]

Proprietary solutions / IP / Products (representative list)

Solutions	Details
Wipro CyberTransform – intelligent risk and security	It is integrated with ServiceNow and provides timely, actionable enterprise risk information in weeks. It contributes to continuous monitoring, increased visibility, and scalable security – all simplified for the modern company. It navigates the digital transformation landscape in an industry-standard manner, assuring quality operations, risk minimization, and regulatory compliance.
Security management center	It identifies operational security concerns throughout the firm.
Decentralized Identity and Credential Exchange ID (DICE ID)	It is a blockchain-enabled platform that assists in the issuance and verification of tamper-proof credentials, with the goal of changing credential exchange for a more reliable and inclusive digital society.
Third-party risk management	It is a rapid and efficient automated process for gathering, validating, and continuously monitoring data, with real-time visibility into danger and risk across all third parties.
Cloud Applications Risk Governance (CARG)	It provides a full overview of your single or many cloud settings. The solution provides a single-pane-of-glass view that integrates the critical information required to assess security threats, risks, and compliance status. Wipro CARG continuously monitors and detects potential risk changes, providing you with real-time monitoring and remediation advice.
Wipro ai360	It brings together all its AI skills, talent, and technology to assist clients in connecting AI across their enterprises.
Enterprise data obfuscation	It is a data masking solution that generates an inauthentic yet structurally comparable version of the actual production data that businesses keep up-to-date. It keeps sensitive data from moving from production environments into non-production, while enabling the usage of realistic data for testing and development. The goal is to safeguard the original data while maintaining a workable backup in case the original data is not needed.
Automated Regulatory Compliance (ArC)	It is connected with ServiceNow and offers tracking of industry-specific compliance through an expanding collection of apps approved by ServiceNow.
Identity management center	It offers a solitary perspective of the IAM environment.

Wipro provider profile – North America (page 4 of 7)

Investments and recent activities

[NOT EXHAUSTIVE]

Investments (representative list)

Investments	Details
Investment	Invested in Vectra to take advantage of its real-time threat hunting and investigation capabilities through AI
Investment	Invested in Vulcan to take use of its platform for fixing vulnerabilities and speed up reaction times
Investment	Invested in Securonix to take advantage of its cutting-edge threat detection and response capabilities for data-driven and hybrid cloud businesses
Investment	Invested in CyCognito to take advantage of its cutting-edge cybersecurity technology, which maps the attack surface of an organization and helps to remove blind spots
Investment	Invested in Qwiet AI to take use of its software composition analysis and static application security testing capabilities to produce a unified picture of vulnerabilities
Investment	Invested in Riscosity for API security

Wipro provider profile – North America (page 5 of 7)

Partnerships

[NOT EXHAUSTIVE]

Partnerships (representative list)

Partners	Partnership type	Details
Microsoft	Technology partnership	As Microsoft's strategic security partner, Wipro offers comprehensive Azure and Microsoft 365 security solutions to shared clients.
Palo Alto Networks	Technology partnership	Wipro and PANW have formed a strategic partnership to optimize network and security operations. By adopting a zero-trust framework, they aim to bolster security posture through prevention, early detection, and rapid response.
AWS	Technology partnership	Wipro, a premier AWS consulting partner, has a dedicated team focused on accelerating client cloud adoption. Through joint go-to-market strategies and custom solution development, Wipro and AWS aim to enhance cloud security.
Google	Technology partnership	Wipro, a Google Cloud premier partner, collaborates with Google on a strategic go-to-market approach. Together, they provide advanced cybersecurity and risk management services.
ZScaler	Technology partnership	Wipro and Zscaler's strategic alliance focuses on delivering integrated solutions for zero-trust, secure access, and multi-cloud security. This partnership involves significant investments and resource allocation to support joint initiatives.
Cycognitov	Technology partnership	Wipro and CyCognito partner to offer automated external attack surface management services, helping organizations identify and mitigate potential security risks through continuous testing and vulnerability management.

Wipro provider profile – North America (page 6 of 7)

Partnerships

[NOT EXHAUSTIVE]










Partnerships (representative list) (Tab 2)

Partners	Partnership type	Details
Checkpoint	Technology partnership	Wipro and Checkpoint partner to provide advanced cloud security solutions, safeguarding enterprise cloud workloads and data from sophisticated cyber threats.
Skybox	Technology partnership	Skybox and Wipro's partnership enhances IT-OT network visibility and security, enabling organizations to effectively manage and protect their complex infrastructure.
CrowdStrike	Technology partnership	Wipro is a managed services partner for CrowdStrike and offers the CrowdStrike platform as part of its end point security solution.
Cyberark	Technology partnership	Wipro and CyberArk have a long-standing Platinum partnership, offering comprehensive Privilege Access Management (PAM) solutions. Together, they provide robust security solutions to protect high-value assets for enterprises and government organizations.
Fortinet	Technology partnership	Wipro and Fortinet have a strategic partnership focused on delivering comprehensive cybersecurity solutions. This collaboration combines Wipro's deep industry expertise and service delivery capabilities with Fortinet's advanced security technologies, providing organizations with robust protection against evolving cyber threats.
Rubrik	Technology partnership	Wipro and Rubrik jointly offer modernized data protection and robust cybersecurity solutions, safeguarding critical applications from ransomware threats across on-premise and multi-cloud environments.

Wipro provider profile – North America (page 7 of 7)

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 compliance, risk, and governance may find Wipro suitable owing to its automation-led compliance services through its Automated Regulatory Compliance (ArC) offering
- Wipro's investment in analytics-driven security, using AI-powered risk and identity behavior analytics, enables it to offer offensive cybersecurity to enterprises
- Wipro's acquisition of Edgile and Ampion along with BFSI specialist Capco has enhanced its industry-specific cybersecurity advisory capabilities especially across IAM and risk, governance, and compliance
- Enterprises seeking end-to-end cybersecurity services may find Wipro to be a pertinent partner of choice with its dedicated System Integration and MSS (SIMS) business unit focused on 360-degree security
- Enterprises have lauded the domain expertise and talent and project management of Wipro

Limitations

- Enterprises from public sector looking for cybersecurity services should be aware that Wipro has a limited market presence in public sector in the region
- Enterprises looking for a robust onshore-nearshore presence may find Wipro lagging its peers in providing a strong localized presence
- A few clients have highlighted that Wipro usually confines itself to the immediate scope of the engagement and does not take proactive measures in pitching innovative IP and solutions
- Wipro lags collaboration with niche technology providers to deliver specialized solutions across different cybersecurity segments
- Enterprises seeking extensive flexibility and customization may encounter limitations in Wipro's offerings, as they primarily rely on standardized solutions

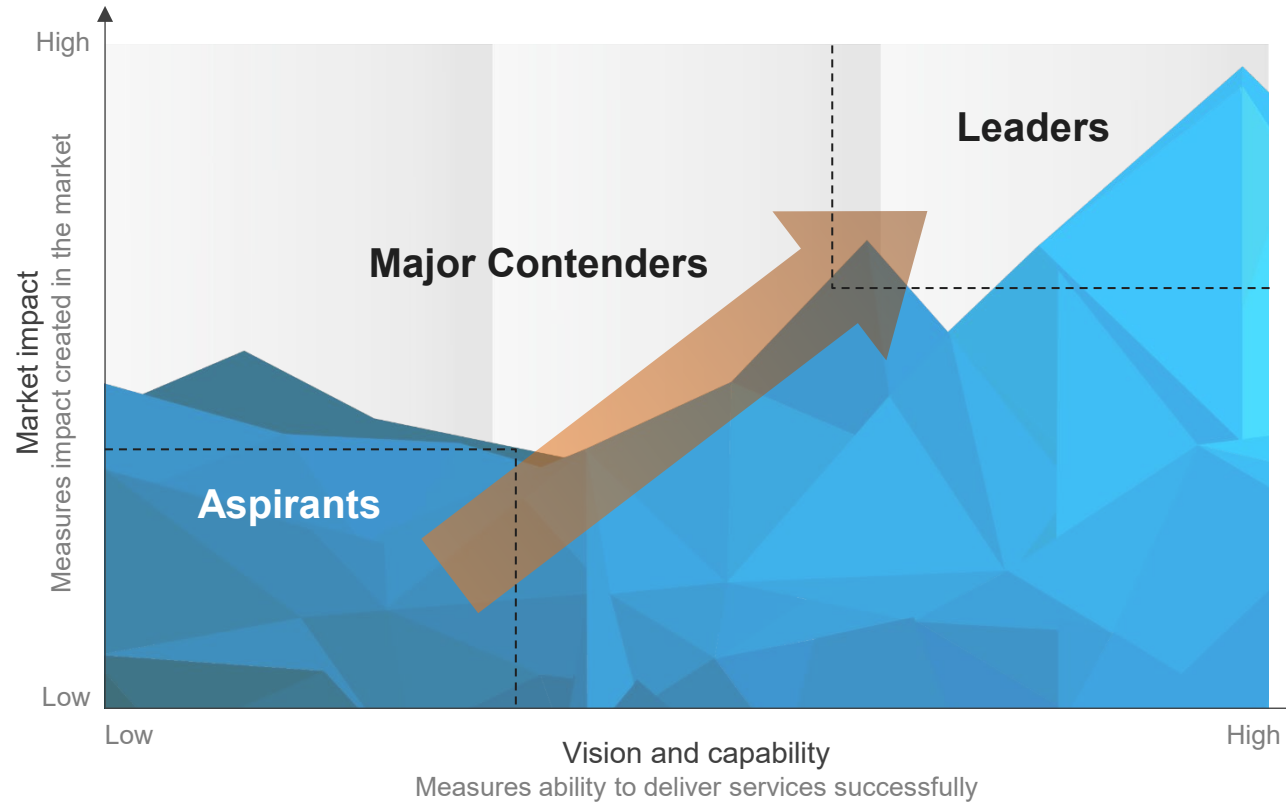
Appendix

PEAK Matrix® framework

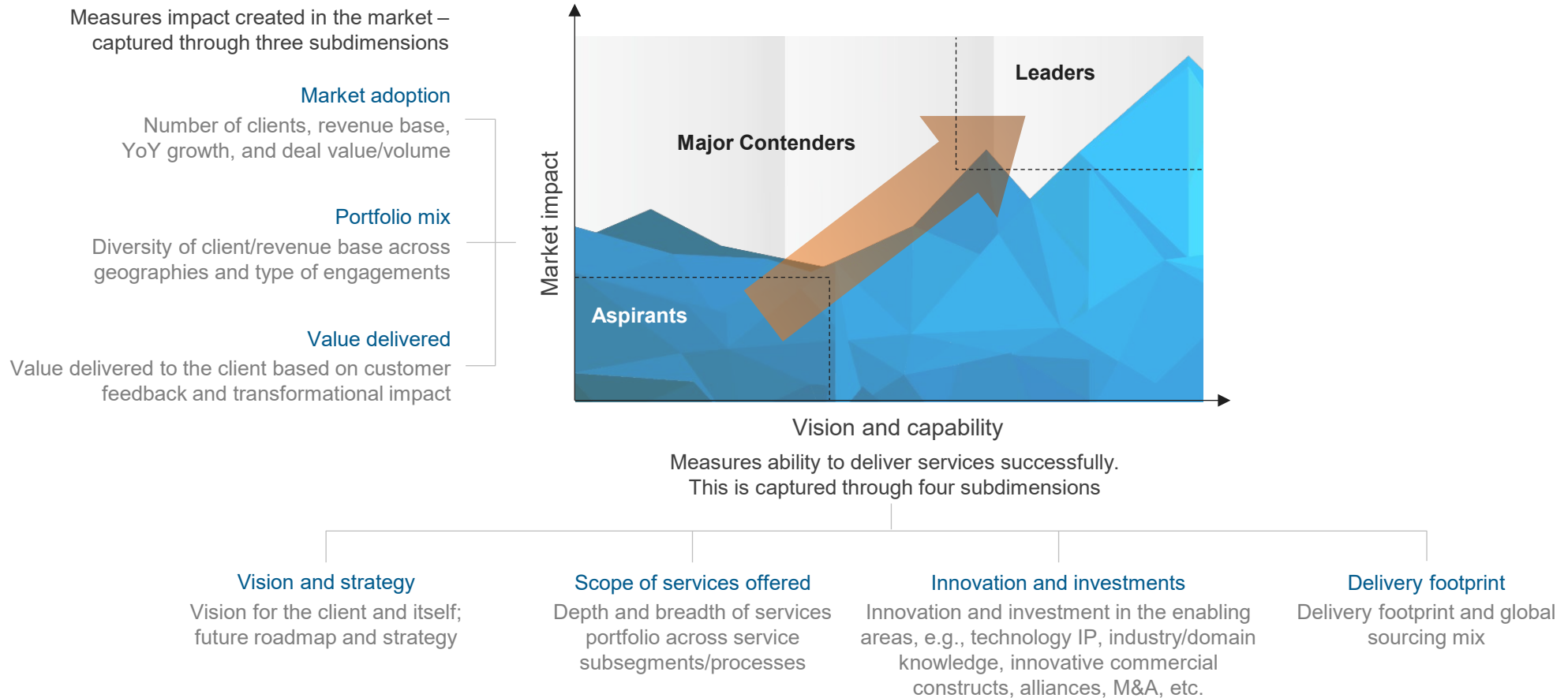
FAQs

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

Everest Group PEAK Matrix



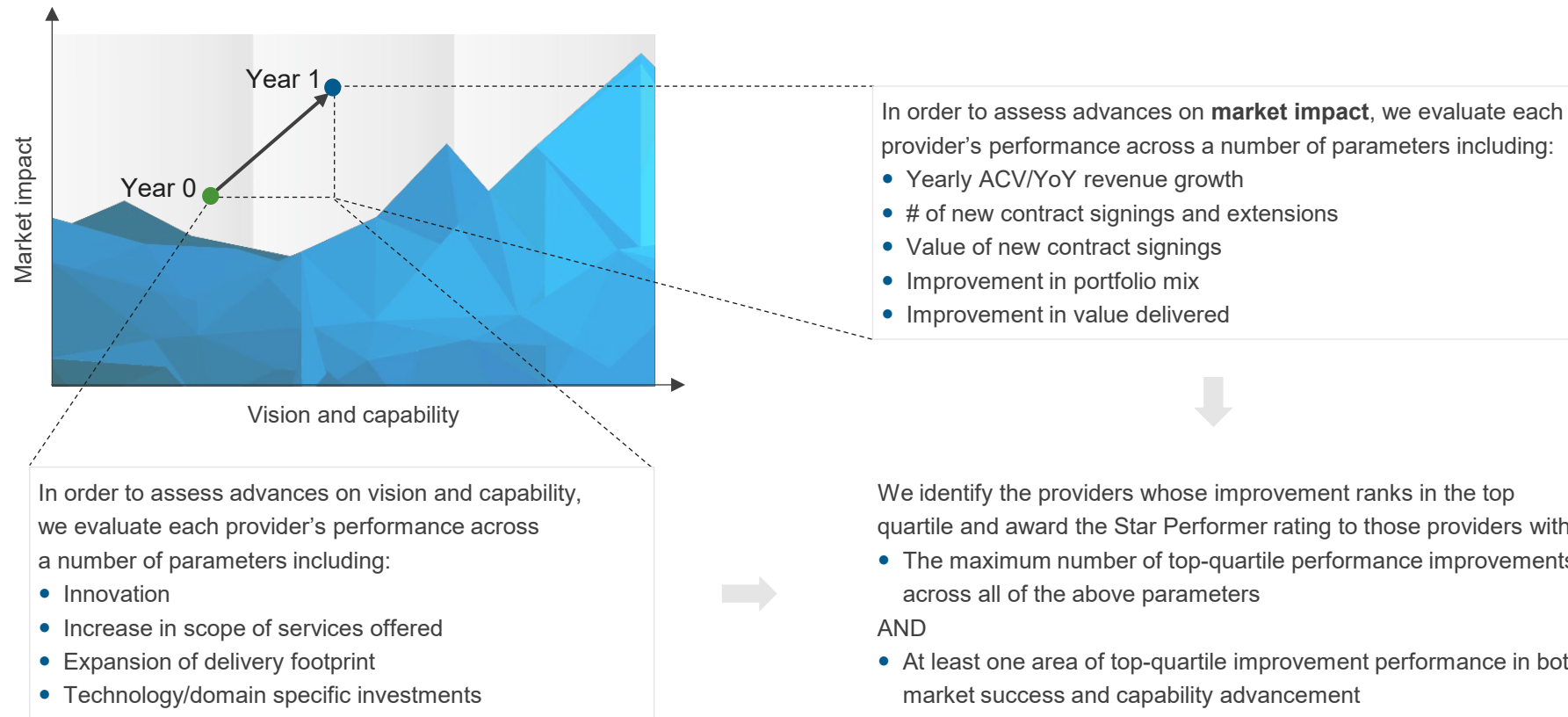
Services PEAK Matrix® evaluation dimensions



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

Methodology

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



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

FAQs

Q: Does the PEAK Matrix® assessment incorporate any subjective criteria?

A: Everest Group's PEAK Matrix assessment takes an unbiased and fact-based approach that leverages provider / technology vendor RFIs and Everest Group's proprietary databases containing providers' deals and operational capability information. In addition, we validate/fine-tune these results based on our market experience, buyer interaction, and provider/vendor briefings.

Q: Is being a Major Contender or Aspirant on the PEAK Matrix, an unfavorable outcome?

A: No. The PEAK Matrix highlights and positions only the best-in-class providers / technology vendors in a particular space. There are a number of providers from the broader universe that are assessed and do not make it to the PEAK Matrix at all. Therefore, being represented on the PEAK Matrix is itself a favorable recognition.

Q: What other aspects of the PEAK Matrix assessment are relevant to buyers and providers other than the PEAK Matrix positioning?

A: A PEAK Matrix positioning is only one aspect of Everest Group's overall assessment. In addition to assigning a Leader, Major Contender, or Aspirant label, Everest Group highlights the distinctive capabilities and unique attributes of all the providers assessed on the PEAK Matrix. The detailed metric-level assessment and associated commentary are helpful for buyers in selecting providers/vendors for their specific requirements. They also help providers/vendors demonstrate their strengths in specific areas.

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

A: Enterprise participants receive summary of key findings from the PEAK Matrix assessment

For providers

- The RFI process is a vital way to help us keep current on capabilities; it forms the basis for our database – without participation, it is difficult to effectively match capabilities to buyer inquiries
- In addition, it helps the provider/vendor organization gain brand visibility through being included in our research reports

Q: What is the process for a provider / technology vendor to leverage its PEAK Matrix positioning?

A: Providers/vendors can use their PEAK Matrix positioning or Star Performer rating in multiple ways including:

- Issue a press release declaring positioning; see our citation policies
- Purchase a customized PEAK Matrix profile for circulation with clients, prospects, etc. The package includes the profile as well as quotes from Everest Group analysts, which can be used in PR
- Use PEAK Matrix badges for branding across communications (e-mail signatures, marketing brochures, credential packs, client presentations, etc.)

The provider must obtain the requisite licensing and distribution rights for the above activities through an agreement with Everest Group; please contact your CD or contact us

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

A: PEAK Matrix assessments are designed to serve enterprises' current and future needs. Given the dynamic nature of the global services market and rampant disruption, the assessment criteria are realigned as and when needed to reflect the current market reality and to serve enterprises' future expectations.

Stay connected

Dallas (Headquarters)
info@everestgrp.com
+1-214-451-3000

Bangalore
india@everestgrp.com
+91-80-61463500

Delhi
india@everestgrp.com
+91-124-496-1000

London
unitedkingdom@everestgrp.com
+44-207-129-1318

Toronto
canada@everestgrp.com
+1-214-451-3000

Website
everestgrp.com

Blog
everestgrp.com/blog

Follow us on



Everest Group is a leading research firm helping business leaders make confident decisions. We guide clients through today's market challenges and strengthen their strategies by applying contextualized problem-solving to their unique situations. This drives maximized operational and financial performance and transformative experiences. Our deep expertise and tenacious research focused on technology, business processes, and engineering through the lenses of talent, sustainability, and sourcing delivers precise and action-oriented guidance. Find further details and in-depth content at www.everestgrp.com.

Notice and disclaimers

Important information. Please review this notice carefully and in its entirety. Through your access, you agree to Everest Group's terms of use.

Everest Group's Terms of Use, available at www.everestgrp.com/terms-of-use/, is hereby incorporated by reference as if fully reproduced herein. Parts of these terms are pasted below for convenience; please refer to the link above for the full version of the Terms of Use.

Everest Group is not registered as an investment adviser or research analyst with the U.S. Securities and Exchange Commission, the Financial Industry Regulatory Authority (FINRA), or any state or foreign securities regulatory authority. For the avoidance of doubt, Everest Group is not providing any advice concerning securities as defined by the law or any regulatory entity or an analysis of equity securities as defined by the law or any regulatory entity.

All Everest Group Products and/or Services are for informational purposes only and are provided "as is" without any warranty of any kind. You understand and expressly agree that you assume the entire risk as to your use and any reliance upon any Product or Service. Everest Group is not a legal, tax, financial, or investment advisor, and nothing provided by Everest Group is legal, tax, financial, or investment advice. Nothing Everest Group provides is an offer to sell or a solicitation of an offer to purchase any securities or instruments from any entity. Nothing from Everest Group may be used or relied upon in evaluating the merits of any investment. Do not base any investment decisions, in whole or part, on anything provided by Everest Group.

Products and/or Services represent research opinions or viewpoints, not representations or statements of fact. Accessing, using, or receiving a grant of access to an Everest Group Product and/or Service does not constitute any recommendation by Everest Group that recipient (1) take any action or refrain from taking any action or (2) enter into a particular transaction. Nothing from Everest Group will be relied upon or interpreted as a promise or representation as to past, present, or future performance of a business or a market. The information contained in any Everest Group Product and/or Service is as of the date prepared, and Everest Group has no duty or obligation to update or revise the information or documentation. Everest Group may have obtained information that appears in its Products and/or Services from the parties mentioned therein, public sources, or third-party sources, including information related to financials, estimates, and/or forecasts. Everest Group has not audited such information and assumes no responsibility for independently verifying such information as Everest Group has relied on such information being complete and accurate in all respects. Note, companies mentioned in Products and/or Services may be customers of Everest Group or have interacted with Everest Group in some other way, including, without limitation, participating in Everest Group research activities.