



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

Focus on Kyndryl
February 2025



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 the 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

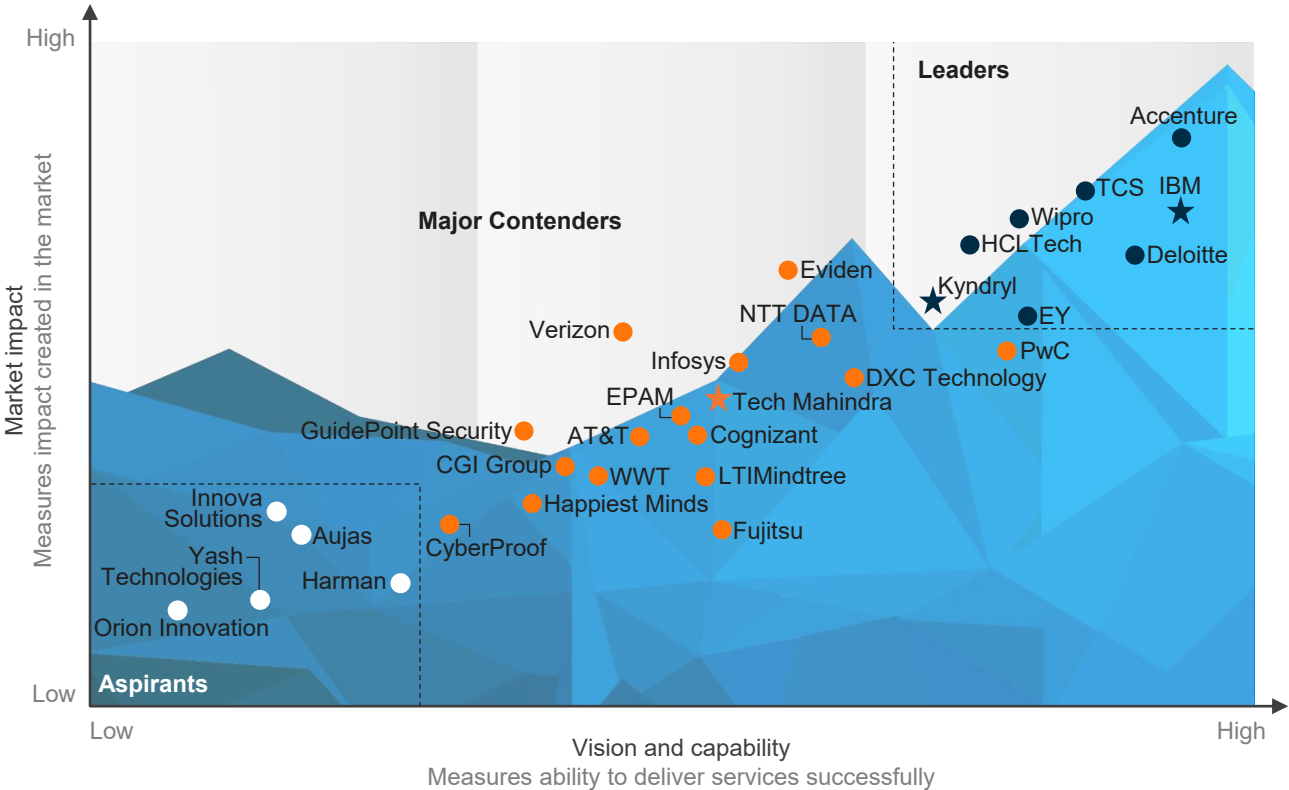
- The cybersecurity business of the Aspirants is still in its early stages and does not cater to large or mega clients in the domain. These providers specialize in limited segments of cybersecurity, offering a narrow scope of services
- These providers are actively broadening their cybersecurity capabilities 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 | Kyndryl is positioned as a Leader and Star Performer

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)

Kyndryl profile (page 1 of 6)

Overview

Vision

Kyndryl assists clients in transitioning from an emphasis on cybersecurity alone to one of cyber resilience, which it describes as the ability to foresee, guard against, withstand, and recover from any adverse circumstance, disruption, or breach of a cyber-enabled organization. Kyndryl helps corporate leaders achieve cyber resilience by combining a consultative approach with the company's established cyber resilience framework and differentiated customer journeys to drive planning, assessments, and engagements toward specified outcomes with quantifiable impact.

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)	● Medium (annual client revenue US\$1-5 billion)	● Large (annual client revenue >US\$5 billion)
--	--	--

Adoption by geography

● United States	● Canada	● Mexico
-----------------	----------	----------

Kyndryl profile (page 2 of 6)

Case studies

CASE STUDY 1

Transformed vulnerability management and PAM for enabling the client's comprehensive protection

Business challenge

The client lacked a consistent vulnerability management solution that could provide full detection and visibility across on-premises and cloud environments, increasing the risk of cyberattacks. Furthermore, its present PAM solution provided insufficient protection for privileged accounts and had inconsistent restrictions.

Solution

Kyndryl partnered with the client to create a rigorous vulnerability management strategy that included complete discovery and visibility of all IT environments. It discovered the existing vulnerabilities and holes in privileged account protection after conducting a full vulnerability gap analysis and PAM workshop. It then created a target state for both vulnerability management and PAM that matched the client's business requirements. The centralized control of the vulnerability management and PAM programs maintained continuous adherence to norms and standards.

Impact

- Increased visibility into program management of both vulnerability management and PAM to reduce the likelihood of a cyberattack
- Assessed tools and recommended which tool to use depending on the company objectives
- Provided a roadmap for improving security posture using a centrally controlled PAM system that aligns with zero trust
- Optimized SOC from the specified strategy

CASE STUDY 2

Enhanced third-party risk management and transformed client operations, streamlining assessment and response efforts

Business challenge

The client manually assessed thousands of third parties, which was both a costly and inefficient exercise. It found it challenging to notify third parties of any vulnerabilities, and therefore, so it remained active. These third parties were examined once a year, or every two or three years, and its security posture varied daily. Third-party risk reporting typically took weeks to complete and was constantly out of date, as the client was unable to analyze third-party risk on a regular basis or resolve vulnerabilities in a timely manner.

Solution

Kyndryl implemented a Third-Party Risk Management (TPRM) solution using Black Kite's platform. This solution provided a transparent cyber ratings platform, offering a 360-degree view of third-party risk. With continuous global scanning based on OSINT and innovative features such as focus tags and workflow engines, the solution was fully scalable and integrated seamlessly with GRC systems.

Impact

- Evaluated thousands of third parties every month
- Increased time-to-awareness and improved informed decision-making by 550 times
- Increased its response to third parties by increasing to publicly announced vulnerabilities by 14 times
- Improved visibility and capacity of reaction with actual relevant reporting by over 20 times
- Reallocated resources from evaluating questionnaires to monitoring and correcting findings with third parties

Kyndryl profile (page 3 of 6)

Solutions

[REPRESENTATIVE LIST]

Proprietary solutions / IP / Products

Solutions	Details
Kyndryl Bridge	It is an open integration platform that gives business leaders control over mission-critical operations and real-time visibility into IT estates. It consists of two main components: a digital console with a unified dashboard that allows clients to easily understand and optimize the existing Kyndryl managed subscriptions and consultations, and a marketplace catalog where customers can browse the available services and request consultations/quotations.
Security Operations-as-a-Platform (SOaaS)	It consolidates security suppliers, reduces attack surfaces, and centralizes technologies. Customers benefit from a single-pane-of-glass view that integrates leading SOAR, SIEM, EDR, and VMS solutions, offering visibility into its security posture and assisting it in making swift data-driven choices.
Kyndryl Bridge CompSecOps	It is a module that provides a holistic view, governance, and remediation across public, private, and hybrid cloud environments to ensure adherence to 44+ regulatory compliance and regimes dispersed across multiple domains such as banking, financial, federal, healthcare, and IT. The dashboard shows what has changed, or drifted, in security risk as well as changes in the asset portfolio. In addition to risk, it provides an overview of changes in compliance posture across several standards such as FISMA, PCI, and FISCAM. AI and ML capabilities are embedded throughout the tool.
Kyndryl Bridge DevSecOps	It is a module that provides a full abstraction of many DevOps technologies, resulting in a unified view of the software development life cycle. It includes comprehensive out-of-the-box connections with DevOps tools and cloud providers, allowing users to rapidly acquire insights into the develop, build, test, and deploy stages using out-of-the-box dashboards. This visibility improves speed and quality. It improves governance by offering customizable security policies that reduce vulnerabilities and increase application quality. Furthermore, the platform enables traceability and transparency using DevOps research agency analytics to improve the development team's velocity and stability.
Kyndryl Resiliency Orchestration	It is a software meant to assist clients in elevating their IT service resiliency from typical server-based recovery, in which Kyndryl recovers the client's storage, servers, and data, to application-defined continuity, in which the client's applications are recovered automatically. One significant advantage is that it allows clients to leverage their existing data replication technologies and consolidate them into a single perspective for better disaster recovery/backup planning.

Kyndryl profile (page 4 of 6)

Investments and recent activities

[REPRESENTATIVE LIST]

Investments

Investments name	Details
Kyndryl Foundation	It established the nonprofit, private Kyndryl Foundation. Grants for community development initiatives are given out by the foundation on the basis of trust. One of the most recent investments made in North America is in CodePath, which reprograms college education to produce a broad pool of engineers, CTOs, and entrepreneurs. The programs it offers include gGirl Security, which promotes cybersecurity career paths for girls, women, and gender minorities aged 14 to 26 from underrepresented communities, and NPower, which aims at developing a diverse workforce by launching digital career opportunities for underserved young adults and military veterans, enabling economic prosperity and helping them succeed in the digital economy. All of these programs have been approved by the industry and are focused on meeting the needs of Black, Latino/a, indigenous, and low-income students.
Co-innovation with partners	It enters into alliances and partners for enabling co-innovation in order to plan, develop, oversee, and update the critical systems of its clients. This was further enhanced by security and resiliency. With the help of Veritas, Rubrik, Cisco, and AWS, it effectively implemented this procedure and introduced new Kyndryl services to the market, and aimed to increase important alliances within the portfolio. It made these collaborations public with the following markets: • Announced a strategic global alliance with Palo Alto Networks to provide network and cybersecurity services • Announced a partnership with Thales for comprehensive response to cybersecurity incidents • Announced an expanded partnership with Cisco focusing on cyber resilience • Announced the global Veeam alliance to deliver comprehensive cyber resilience security and resilience; it collaborated with partners to create new Kyndryl solutions and services • Revealed new Veritas data protection and recovery technologies • Announced a partnership on the cyber threat intelligence platform with AWS • Partnered with Cisco to launch new security service edge and SASE capabilities
Talent	It made investments with a focus on staff retention and bringing in new hires to grow into areas that matter to its clients. It invested significantly to draw in new, seasoned professionals who expanded its wallet share and presence at its current accounts in addition to bringing in new branded clients. Kyndryl also prioritized preparing its practitioners to manage the constantly changing threat landscape in IT systems. Kyndryl's constant upskilling keeps its service delivery process evolving and transforming. This covers certification pathways, partner training, and external training programs in addition to internal training initiatives.

Kyndryl profile (page 5 of 6)

Partnerships

[REPRESENTATIVE LIST]

Partnerships

Partners	Partnership type	Details
AWS	Technology partnership	Kyndryl partnered with AWS to co-create a new security operations platform and threat insights on AWS by utilizing AWS Security Lake and AWS Data.
Microsoft	Technology partnership	Kyndryl partnered with Microsoft on co-innovation, co-investment, and EDR (Microsoft Defender) and cyber incident recovery using Azure in the areas of SIEM and SOaaS (Microsoft Sentinel).
Palo Alto Networks	Technology partnership	Kyndryl partnered with Palo Alto Networks on security operations and response services and SOaaS.
Cisco	Technology partnership	Kyndryl collaborated with Cisco to provide a combined solution for Cisco SSE. Kyndryl Managed SSE with Cisco Secure Access offers a modular and unified way to managing an SSE infrastructure. Kyndryl, in conjunction with its SSE advisory and implementation services, provides help throughout the SSE solution life cycle, from design and implementation to continuing administration. Managed SSE services are meant to assist enterprises in managing and monitoring an SSE solution depending on their specific business needs.
Rubrik	Technology partnership	Kyndryl Incident Recovery with Rubrik is a fully managed, comprehensive, and secure as-a-service solution that provides end-to-end data security by including cyber incident recovery, backup and restore, and continuous data replication. This dependable and scalable solution manages massive enterprise data protection and rapid recovery, and enables businesses to drastically decrease the effect of cyberattacks and return to business.
Veeam	Technology partnership	Kyndryl Managed Backup Services with Veeam is a backup solution made available to customers in collaboration with Veeam. This technology is extremely scalable and serves both enterprise and mid-market customers.

Kyndryl profile (page 6 of 6)

Everest Group assessment – Leader and Star Performer

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 pure-play zero-trust-as-a-service may find Kyndryl to be a suitable fit due to its balanced offerings including zero-trust consulting and managed services for IT/OT convergence
- Enterprises searching for disaster recovery services may find Kyndryl to be a pertinent choice with its hybrid cloud recovery services offerings such as Disaster Recovery-as-a-service and Resiliency Work Area Recovery Managed Services
- Kyndryl may be a relevant choice for enterprises looking for cost-optimized, managed security services as it can provide automation-embedded and platform-delivered services through the Kyndryl Bridge offering
- Kyndryl has invested in partnership alliances allowing it to provide co-innovative solutions such as incident response with Thales and data security with Veritas
- Enterprises seeking global cybersecurity services may appreciate Kyndryl's onshore, offshore, and nearshore presence

Limitations

- Enterprises should evaluate Kyndryl's capabilities as it lags its peers in enterprise mindshare in OT security services due to limited investment in innovative solutions
- Enterprises should carefully evaluate Kyndryl for application security services as it lags its peers in developing a strong suite of frameworks and accelerators
- Some clients have raised concerns about Kyndryl lagging peers in effectively communicating cybersecurity implications to senior business stakeholders
- A few clients have highlighted that Kyndryl needs to be more proactive in suggesting Kyndryl platforms and IP
- Small enterprises should be aware of Kyndryl's focus on midsized and large clients that can impact their domain expertise

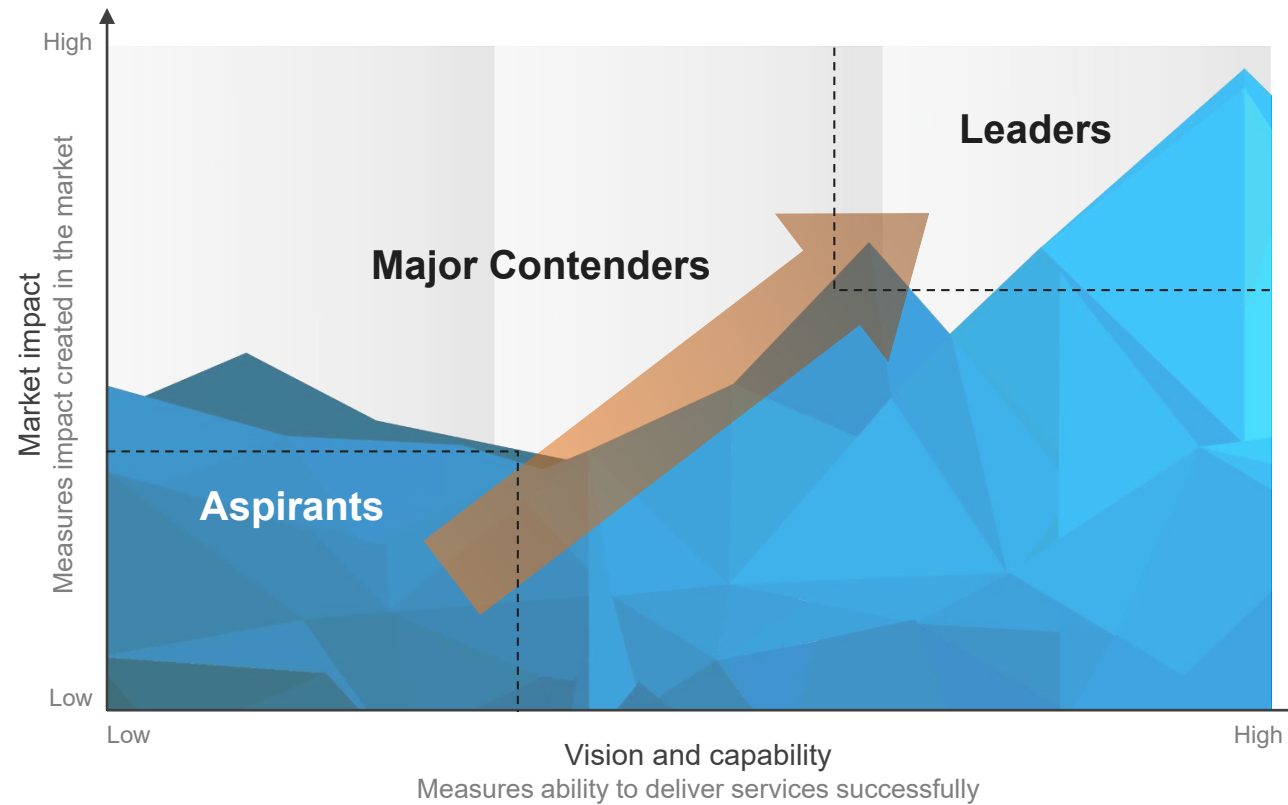
Appendix

PEAK Matrix® framework

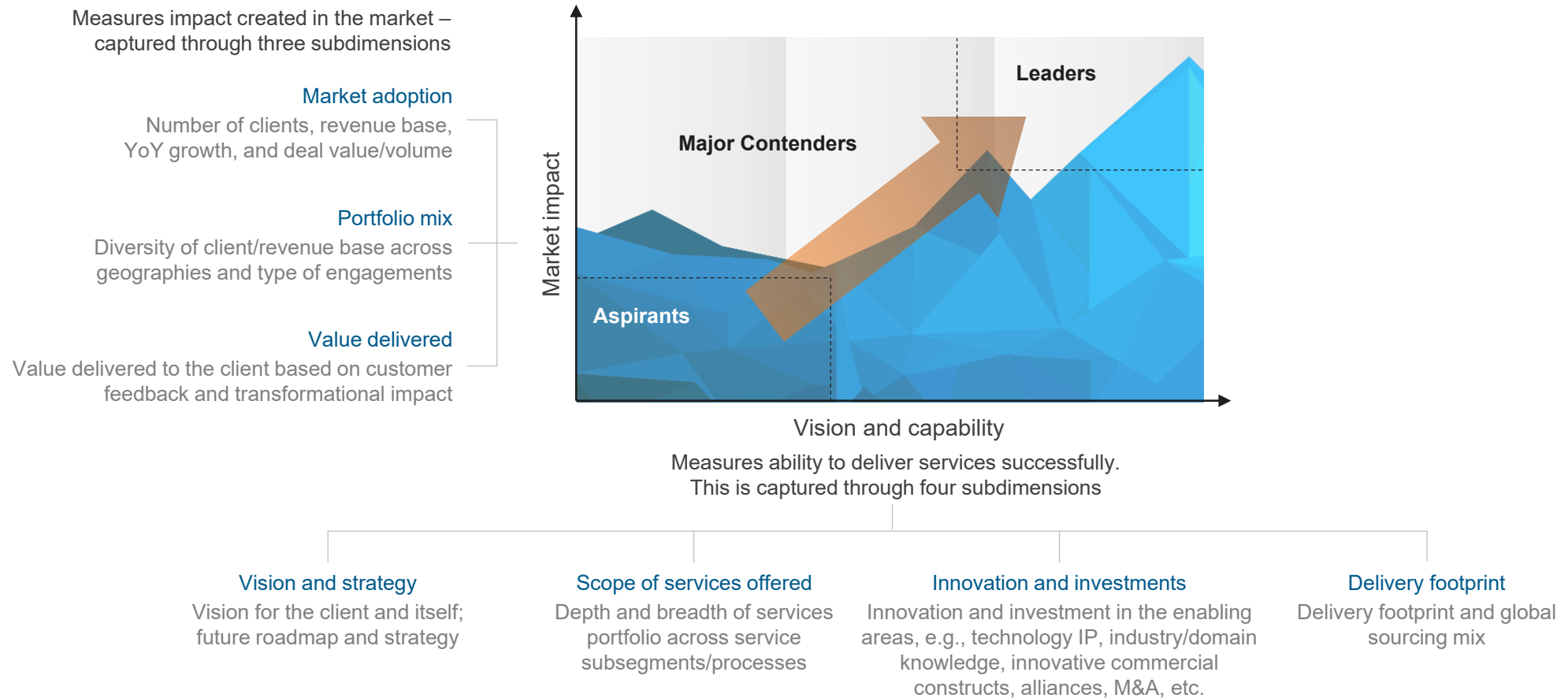
FAQs

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

Everest Group PEAK Matrix



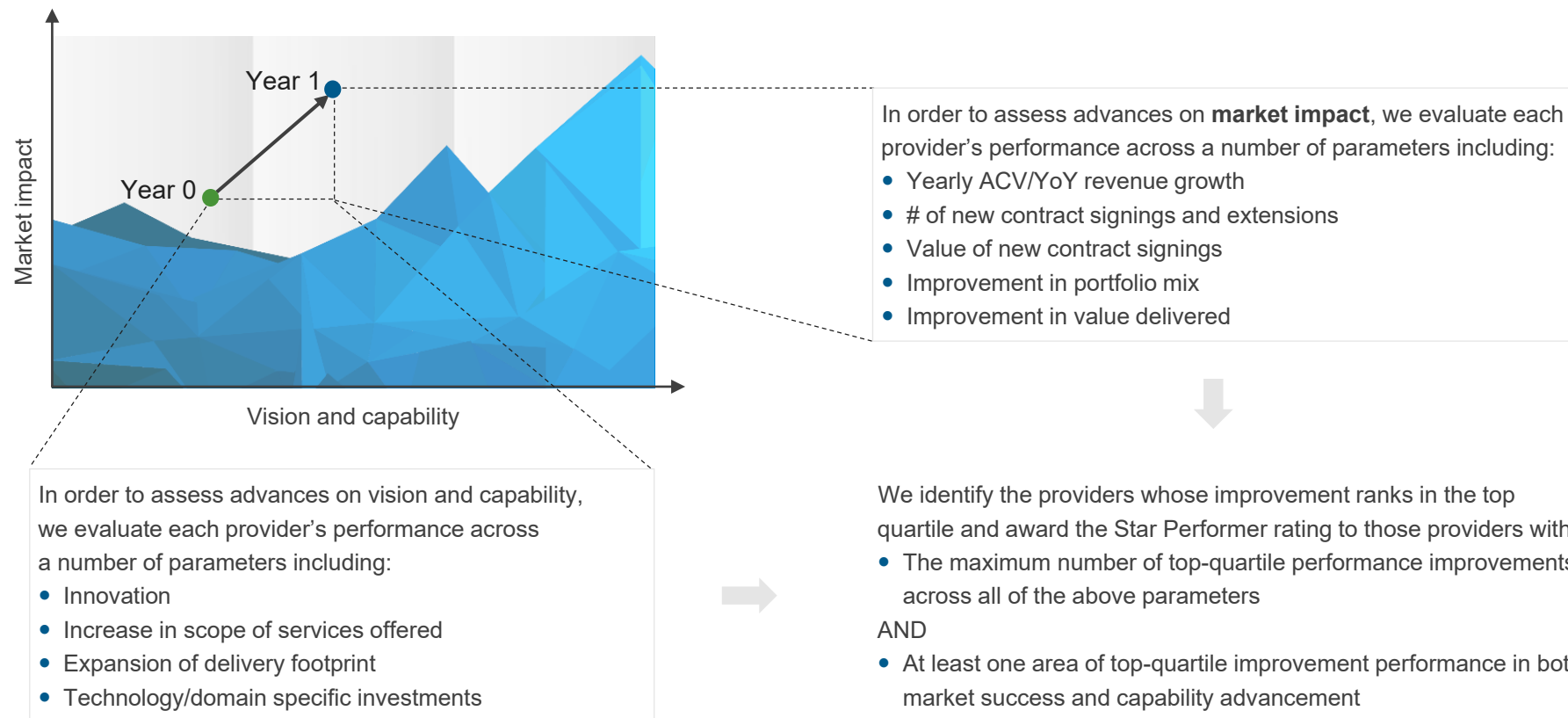
Services PEAK Matrix® evaluation dimensions



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 read this notice carefully and in its entirety. By accessing Everest Group materials, products or services, 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 the Terms of Use are shown below for convenience only. Please refer to the link above for the full and official 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 Regulation Authority (FINRA), or any state or foreign (non-U.S.) 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 properties, assets, materials, products and/or services (including in relation to Gen AI) of Everest Group are provided or made available for access on the basis such is for informational purposes only and provided "AS IS" without any warranty of any kind, whether express, implied, or otherwise, including warranties of completeness, accuracy, reliability, noninfringement, adequacy, merchantability or fitness for a particular purpose. All implied warranties are disclaimed to the extent permitted by law. You understand and expressly agree that you assume the entire risk as to your use and any reliance upon such.

Everest Group is not a legal, tax, financial, or investment adviser, 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.

Everest Group materials, products and/or services represent research opinions or viewpoints, not representations or statements of fact. Accessing, using, or receiving a grant of access to Everest Group materials, products and/or services does not constitute any recommendation by Everest Group to (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 material, 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 collects data and information from sources it, in its sole discretion, considers reliable. Everest Group may have obtained data or information that appears in its materials, products and/or services from the parties mentioned therein, public sources, or third-party sources, including data and information related to financials, estimates, and/or forecasts. Everest Group is not a certified public accounting firm or an accredited auditor and has not audited financials. Everest Group assumes no responsibility for independently verifying such information.

Companies mentioned in Everest Group materials, 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.

