



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

Focus on Accenture

September 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

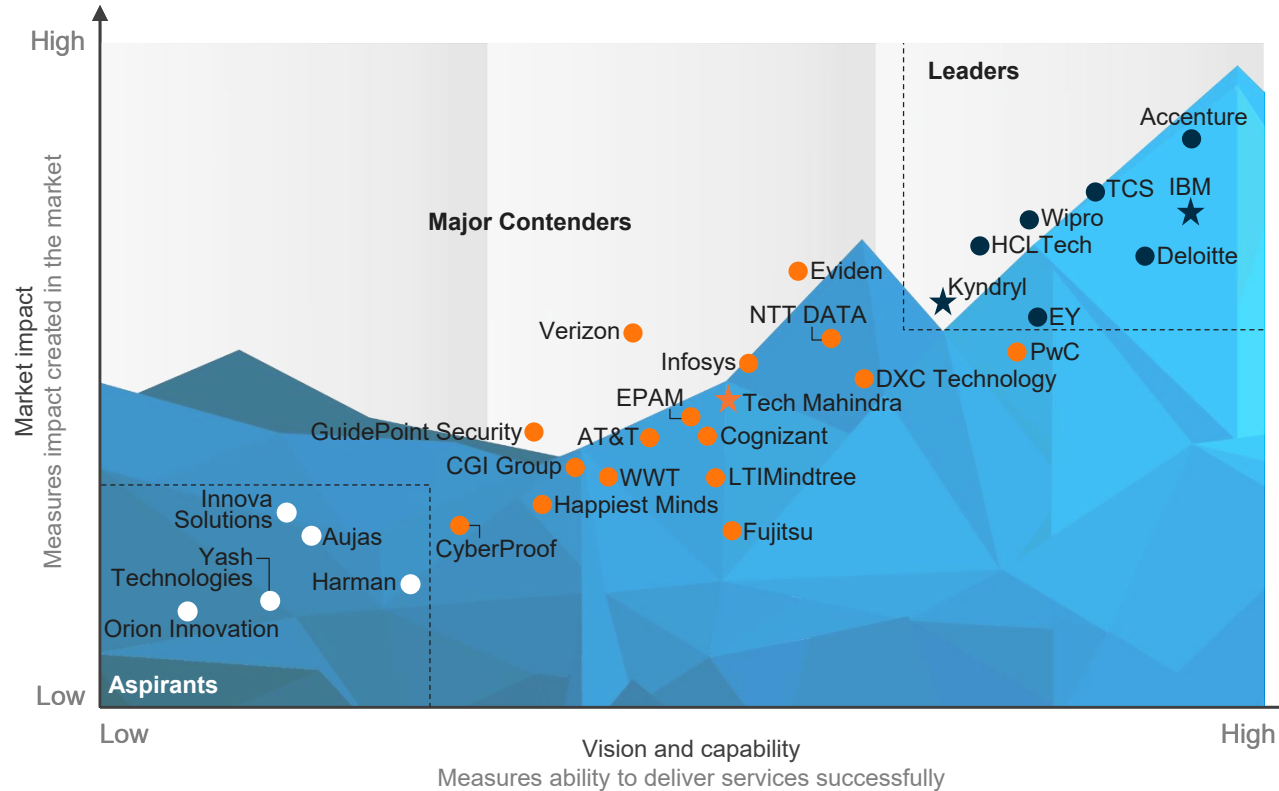
- The cybersecurity business of the Aspirants is still in its early stages and does not cater to large or mega clients in the domain. These providers specialize in limited segments of cybersecurity, offering a narrow scope of services
- These providers are actively broadening their cybersecurity capabilities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

Accenture profile – North America (page 1 of 8)

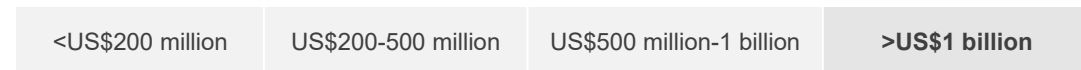
Overview

Vision

Accenture’s global security vision is to be the leading partner for an evolving cyber-resilient business and embed best-in-class cybersecurity capabilities in everything it delivers. It helps clients execute cybersecurity as a business priority to enable growth, protect client’s business and position them for the future. Through highly-differentiated security services, Accenture delivers 360° business value to clients, stakeholders and community. Accenture provides asset-led, industry-driven security solutions at speed and scale, leveraging onshore & offshore expertise, and innovative, collaborative approaches with clients. With security now the top global business risk and a component of ESG investments, Accenture’s vision influences how organizations view cybersecurity by emphasizing that it is a business imperative and a key enabler to organizational growth, stability and competitiveness –not just a technical function.

Accenture is committed to integrating generative AI into its cybersecurity service delivery. This asset-led approach aims to expedite value realization and enhance outcomes for clients.

Cybersecurity services revenue – North America (CY 2024)



● 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

Accenture profile – North America (page 2 of 8)

Case studies

[NOT EXHAUSTIVE]

CASE STUDY 1

Making cybersecurity an enabler of business growth and expansion

Client: a global clinical trial and life sciences research organization

Business challenge

The client, a forward leaning global clinical trial and life sciences research organization, sought to differentiate itself from competitors by focusing on the creation and delivery of high-quality data-driven research outcomes and health-related insights at a speed that would disrupt the market. Its data-centric approach required understanding and adherence to evolving data-related industry and government regulations worldwide. Additionally, it required the flexibility to seamlessly integrate acquisitions. It concluded that its advanced data centric business would require a new generation of cyber resilience strategy and operations to protect the company and its patients, while facilitating expansion into new markets. It also recognized the importance of partnering with a company that has a deep understanding of the life sciences industry and the global regulatory environment and holds the necessary skills and expertise to bring its plan to life.

Solution

Accenture was selected to co-create, architect, and operate its new global cybersecurity operations from the ground up. It provided the full breadth of capabilities from build to managed services and across all security functions including security operations, threat intelligence, vulnerability management, identity, risk and compliance, and employee education.

Impact

- The partnership supported the client's shift to a data-centric approach for business growth, leveraging flexible risk and security strategies. It also established a cybersecurity program that enabled the client to maintain resilience and compliance with security best practices and regulations
- Rather than purchasing and overseeing generic third-party services, the client became an intentional user of expert integrated managed services purposefully architected to support its business plan

CASE STUDY 2

Bringing innovation, continuous improvement, and flexibility to lead the client through the next chapter of its security journey

Client: a global 500 conglomerate

Business challenge

The client, a multi-industry conglomerate planning to execute a series of large global divestitures as part of a strategic business realignment, sought to guard shareholder value before, throughout, and post transaction by ensuring consistently high levels of cybersecurity threat protection and resilience were maintained throughout the process. The client knew the right partner would bring global scale and depth and breadth of knowledge across cybersecurity domains – especially digital identity and threat and vulnerability management, the programs for which included legacy tools, custom developed software, and involved support from multiple niche subcontractors. The client also faced increasing levels of cybersecurity employee departures.

Solution

Accenture was selected to take over, reimagine, and deliver back to the client digital identity and threat and vulnerability operations as-a-service, globally. As part of the execution, Accenture leveraged its vast reach and depth of expertise to take direct responsibility for work previously performed by dozens of subcontractor companies, rapidly filled resource gaps, and introduced proven Accenture methods and tools that improved consistency and quality of operations.

Impact

- Operating more securely (improved security posture), with greater confidence, and solid processes in place
- Lower cost than if work was handled internally
- Optimized delivery teams and expanded the scope of identity services across the corporate footprint
- Helped build resiliency across Identity as attrition ramped up
- Started to expand Identity services to other spin-off companies

Accenture profile – North America (page 3 of 8)

Solutions

[REPRESENTATIVE LIST] [NOT EXHAUSTIVE]

Proprietary solutions / IP / Products

Solutions	Details
mySecurity	Accenture Security's portfolio of services is powered by mySecurity, its suite of gen AI-powered assets, leveraging partner technology, that is designed to optimize the security foundation end-to-end, lower operating costs, modernize faster, and improve cyber resilience.
Cyber Industry	Build resilience and mitigate risk across each industry's value chain covering Communication, Media, and Technology (CMT), products, health and public service, financial services, and resources. Embed security to build cyber resilience and mitigate cyber risk across critical areas of each industry's value chain, with solutions tailored to industry-specific needs, regulations, and rules
Cyber Protection	<ul style="list-style-type: none"> Protect the business as it transforms – applying zero trust principles to secure the entire digital core including cloud, data, AI, enterprise platforms, applications, access and emerging technologies mySecurity assets and accelerators: mySecurity for identity and access management; mySecurity for applications; mySecurity for cloud; mySecurity diagnostic for AI and data; mySecurity for zero trust, network and SASE and cybersecurity mesh; mySecurity for enterprise platform security
Cyber Resilience	<ul style="list-style-type: none"> Pressure test defenses, understand emerging threats, and prepare and respond quickly to attacks; includes offerings around cyber defense, cyber response and cyber intelligence mySecurity assets and accelerators: mySecurity for threat detection and response; mySecurity Portal for managed security services; mySecurity for cyber defense; mySecurity for cyber intelligence; mySecurity for cyber response; mySecurity Diagnostic for Cyber Resilience (CRD).
Cyber Strategy	<ul style="list-style-type: none"> Design and operationalize cyber risk strategies to protect and accelerate transformations and enable customer trust. Includes offerings around c-suite and board cyber advisory, cyber risk and regulatory, security strategy and organization, and cyber risk and compliance as-a-service mySecurity assets and accelerators for cyber strategy: cost optimization security tooling assessment; cyber resilient CEO benchmarking assessment; geopolitical cyber risk assessment, and security maturity assessment
Cyber-physical Security	<ul style="list-style-type: none"> Protect operational reliability and integrity by securing industrial control systems and connected products at all stages of their life cycle. mySecurity assets and accelerators: mySecurity for operational technology security; product security assessment; mySecurity for threat detection and response; mySecurity portal for managed security services; mySecurity for cyber response

Accenture profile – North America (page 4 of 8)

Investments, and recent activities

[REPRESENTATIVE LIST] [NOT EXHAUSTIVE]

Investments

Investments name	Details
Acquisition	Mnemo Mexico: managed security services, cyber defense intelligence services
Investments in startups	<ul style="list-style-type: none"> • Tenchi Security: third-party cyber risk management – SaaS platform connecting clients with their supply chains • Interos: AI SCRM platform – detect and correct supply chain non-conformance in real time • SpiderOak – secure satellite communications in space • Aliro Quantum – equip clients with secure quantum networks that establish safe and secure data and communications • QuSecure: cybersecurity in orbit – after collaboration Accenture accomplished the first successful multi-orbit data communications test secured with Post-quantum Cryptography (PQC)
Talent	<ul style="list-style-type: none"> • NA apprenticeships: aiming to grow future security leaders in North America • Internal upskilling programs (e.g., ACES Up and CyberHer) • Leadership development programs: security participants in all Accenture leadership development and coaching programs e.g., Leadership Credential, Insights – Diverse Leadership Development, BetterUp Coaching, and Executive Coaching
\$3 billion investment over three years in gen AI	<ul style="list-style-type: none"> • Accenture will double AI talent to 80,000 people through hiring, acquisitions, and training • Accenture’s AI expertise includes more than 1,570 patents, encompassing pending patents on applications worldwide, and hundreds of scaled client solutions. Expanded Data & AI practice will offer new industry solutions and pre-built models that will help companies across 19 industries drive value • The Center for Advanced AI is dedicated to maximizing the value of this technology across clients and within Accenture. This includes extensive R&D and investments to reimagine service delivery using generative and other emerging AI capabilities. • Accenture will invest in new and existing relationships across its industry-leading cloud, data, and AI ecosystems

Accenture profile – North America (page 5 of 8)

Investments, and recent activities

[REPRESENTATIVE LIST] [NOT EXHAUSTIVE]

Investments

Investments name	Details
Gen AI Security	<ul style="list-style-type: none"> • Accenture established a global Gen AI Security Engineering Hub where they are actively building assets and prototypes to enhance cybersecurity operations powered-by gen AI solutions. Accenture’s gen AI-powered security solutions lower the skill gap for cybersecurity professionals, enhance security context for identified threats, automate security processes to reduce manual labor and create actionable insights, which allow cybersecurity professionals to focus on more complex threats, and to accelerate response time • Accenture evaluates the compatibility of its ecosystem partners’ solutions within its generative AI security lab. Many assets are developed collaboratively with clients and relevant Accenture Security Offering Leaders. This process enables Accenture to swiftly test, refine, and validate the value of assets for clients while also considering their potential integration into the broader portfolio • Accenture Security fosters business use case validation through a secure-by-design methodology. Its services encompass governance, cyber protection, and cyber defense to safeguard organizations and mitigate threats via accelerators, assets, and ecosystem partners • Recent assets include mySecurity for AI Diagnostic, Deepfake Mitigation, AI SOC Assistant, Malware Analysis Automation, Report Generation and Translation, Continuous Compliance, Information Security Standards Search, AI Code Reviewer, IAM Assistant, Secure Cloud Express Delivery Assistant, and Secure Enclave IaC
Quantum Security + SANDBOX AQ	<ul style="list-style-type: none"> • Quantum readiness: assess the threat from quantum, define and modernize the security program, and capabilities and controls framework to enable secure post-quantum transformation • Crypto agility: deploy security controls and capabilities leveraging automation and crypto agility services where possible for continuous compliance • Post-quantum crypto: upgrade infrastructure and tools and begin installation for coming NIST post-quantum cryptography standards; enable business-aligned reporting and response
Space Technology Security	<p>Accenture has invested in building a security testing satellite, the CARET 1. The satellite will be launched to the International Space Station (ISS) later this year and from there pushed into Low Earth Orbit by an ISS astronaut to provide testing capabilities for quantum security as well as identity and access management in space, patch management in space and encryption management into crypto agility in space. Accenture will conduct its own experiments. This is the initial launch in a series of annual launches aimed at increasing capabilities in space. Through this satellite, Accenture is introducing cybersecurity into cyberspace.</p>

Accenture profile – North America (page 6 of 8)

Partnerships

[REPRESENTATIVE LIST] [NOT EXHAUSTIVE]

Partnerships

Partners	Partnership type	Details
AWS	Technology partnership	Working together on AWS' security offerings through Accenture AWS Business Group and directly with the AWS product teams (e.g., Control Tower and Security Hub). Accenture is a launch partner for offerings such as the AWS Network Firewall, Accenture Flywheel, and continuous leverage of its new Security Lake, Bedrock, gen AI, and its new compliance product
CyberArk	Technology partnership	Collaborating on a joint innovation agenda to co-create assets supporting digital identity and privileged access management services
Cloudflare	Technology partnership	Strengthening the ability to detect, prevent, and respond to infrastructure threats through Accenture's Cloudflare Service Capability, providing advisory, deployment, health checks, and managed services
Claroity	Technology partnership	Collaborating on implementation, testing, and configuration to secure connected devices and embedded systems to enable intelligent, connected, and trusted products and services
Crowdstrike	Technology partnership	Collaborating on multiple security offerings across the platform including incident response and recovery, cloud security, data security, identity, MxDR, SOC transformation, and several multi-partner solutions
Fortinet	Technology partnership	Developing joint assets to provide comprehensive security solutions for protection across cloud environments, data centers, connected devices, and Operational Technology (OT) networks
Google Security	Technology partnership	(Cloud, Chronicle, Mandiant) Partnering with Google Cloud to help businesses better protect critical assets and strengthen security by providing the expertise organizations need to build security programs and maintain confidence in their readiness. The partnership includes running Accenture's MxDR platform on Google Chronicle. In 2024, Accenture launched a partnership with Mandiant on Threat Intelligence
Microsoft	Technology partnership	Collaborating with Microsoft product engineering teams to influence roadmaps, co-develop differentiated assets, and productize services including cloud security quick start, security automation, modern identity, proactive compliance, secure on sap, and operations optimization
Nozomi Networks	Technology partnership	Partnering to create a comprehensive OT Security solution to make sure clients are supported throughout their cyber security solution implementation

Accenture profile – North America (page 7 of 8)

Partnerships

[REPRESENTATIVE LIST] [NOT EXHAUSTIVE]










Partnerships

Partners	Partnership type	Details
Okta	Technology partnership	Utilizing preconfigured use cases and rapid application onboarding to design and implement Identity and Access Management (IAM) services capable of securing client environments and experiences
Palo Alto Networks	Technology partnership	Accelerating business transformations while improving network performance, ensuring simpler and consistent security, accelerating time to market, and reducing costs. Accenture and Palo Alto Networks are collaborating to deliver joint Secure Access Service Edge (SASE) solutions powered by Palo Alto Networks® AI-powered Prisma® SASE
Ping Identity/ForgeRock	Technology partnership	Providing digital identity and autonomous identity services; Accenture offers templates across the delivery cycle and an app onboarding accelerator
SailPoint	Technology partnership	Designing and implementing Identity and Access Management (IAM) services. Accenture offers accelerators and IP including 20+ pre-configured use cases, app onboarding accelerator, and an event bridge accelerator
SandboxAQ	Technology partnership	Partnering to deliver Artificial Intelligence (AI) and quantum computing solutions to help organizations identify and remediate cybersecurity vulnerabilities
Saviynt	Technology partnership	Designing and implementing IAM services; joint assets include an application onboarding tool and a test automation suite
ServiceNow	Technology partnership	Building, installing, configuring, and testing of OT stacks through Accenture's ServiceNow Labs and Cyber Fusion Centers
Cisco/Splunk	Technology partnership	Developing joint assets, offerings, and accelerators to help clients improve cyber defense capabilities and overall security posture
Zscaler	Technology partnership	Addressing large-scale customer needs and providing advanced solutions and customer support in the Zero Trust security space through our end-to-end project and delivery capability
Others	Technology partnership	AppOmni, Cyware, HashiCorp, Hyperproof, Interos, Onapsis, One Identity, Open Text, Oracle, Immersive Labs, Rubrik, PlainID, Qualys, Ripjar, Salesforce, SAP, Securiti.ai, Symmetry Systems, Tanium, Thales, and VMWare

Accenture profile – North America (page 8 of 8)

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

- Accenture’s mySecurity platform for threat detection and response along with MxDR embedded with SOC AI assist enables it to provide comprehensive and cost-optimized cybersecurity services to its clients
- Accenture's ability to interpret new regulations and transform business requirements into technical controls using gen AI makes it a pertinent partner for enterprises seeking GRC services
- Enterprises seeking security consulting may find Accenture to be a suitable partner, offering IP-backed services that deliver value realization and Return on Investment (RoI) on cybersecurity investments
- Enterprises from HLS and energy and utility vertical may consider Accenture a long-term partner due to its investments in next-generation security services such as quantum security, gen AI, and SASE
- Some clients have appreciated Accenture for its OT security capabilities

Limitations

- Enterprises looking for localized SOC services may find Accenture lagging compared to peers due to its offshore SOC-focused approach
- Enterprises must be wary that Accenture has limited presence in industries such as BFSI and manufacturing compared to peers
- While clients have praised Accenture's technical capabilities, they expect better strategic-level assistance in cybersecurity
- Some clients have raised concerns about the need for simplification of threat reporting
- Clients have noted the limited visibility of Accenture’s platforms and IP and expect offensive education on these internal solutions

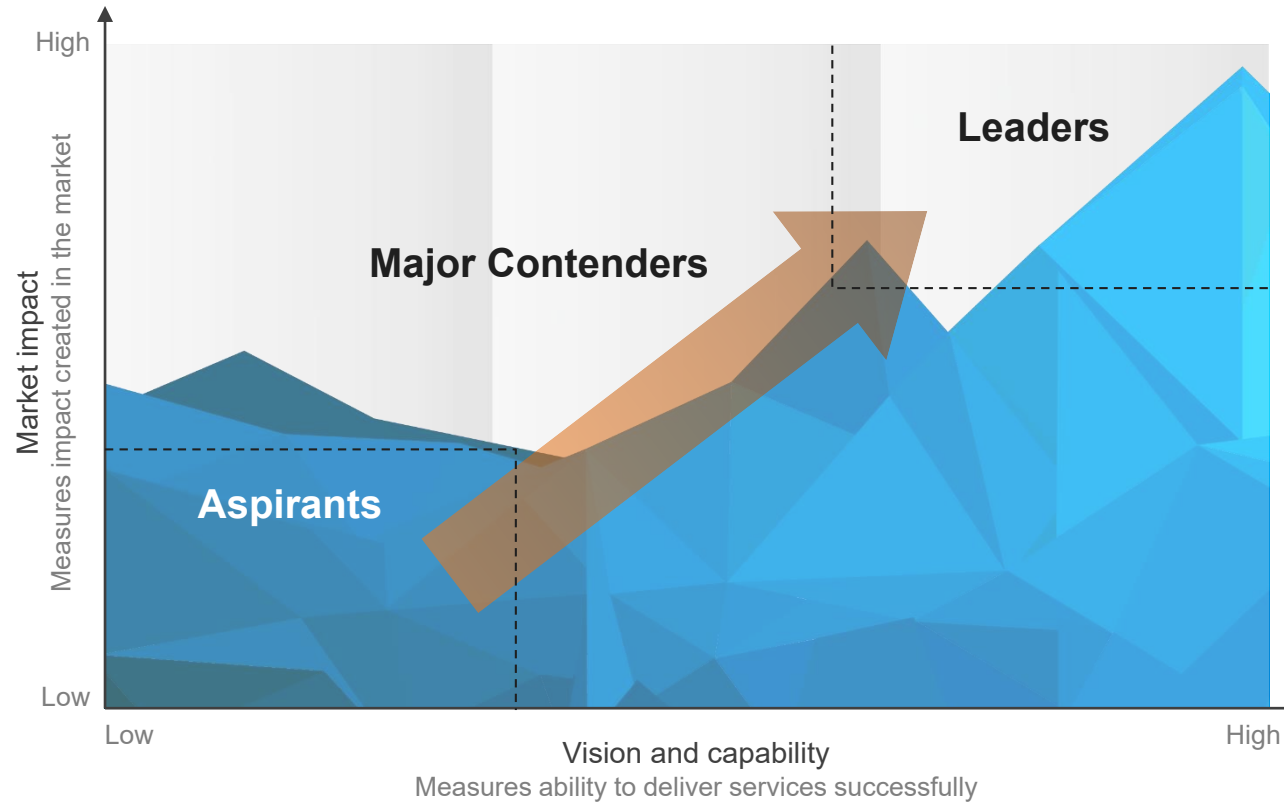
Appendix

PEAK Matrix® framework

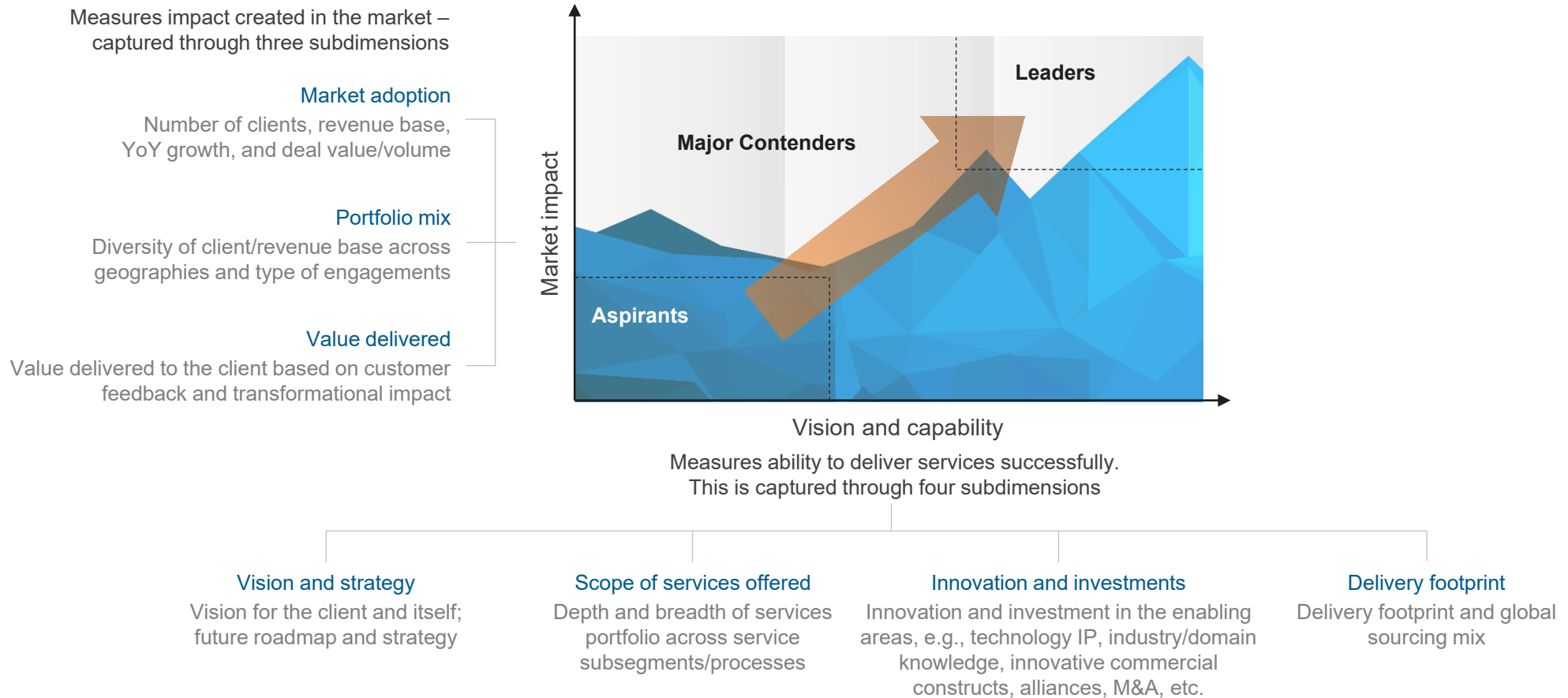
FAQs

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

Everest Group PEAK Matrix



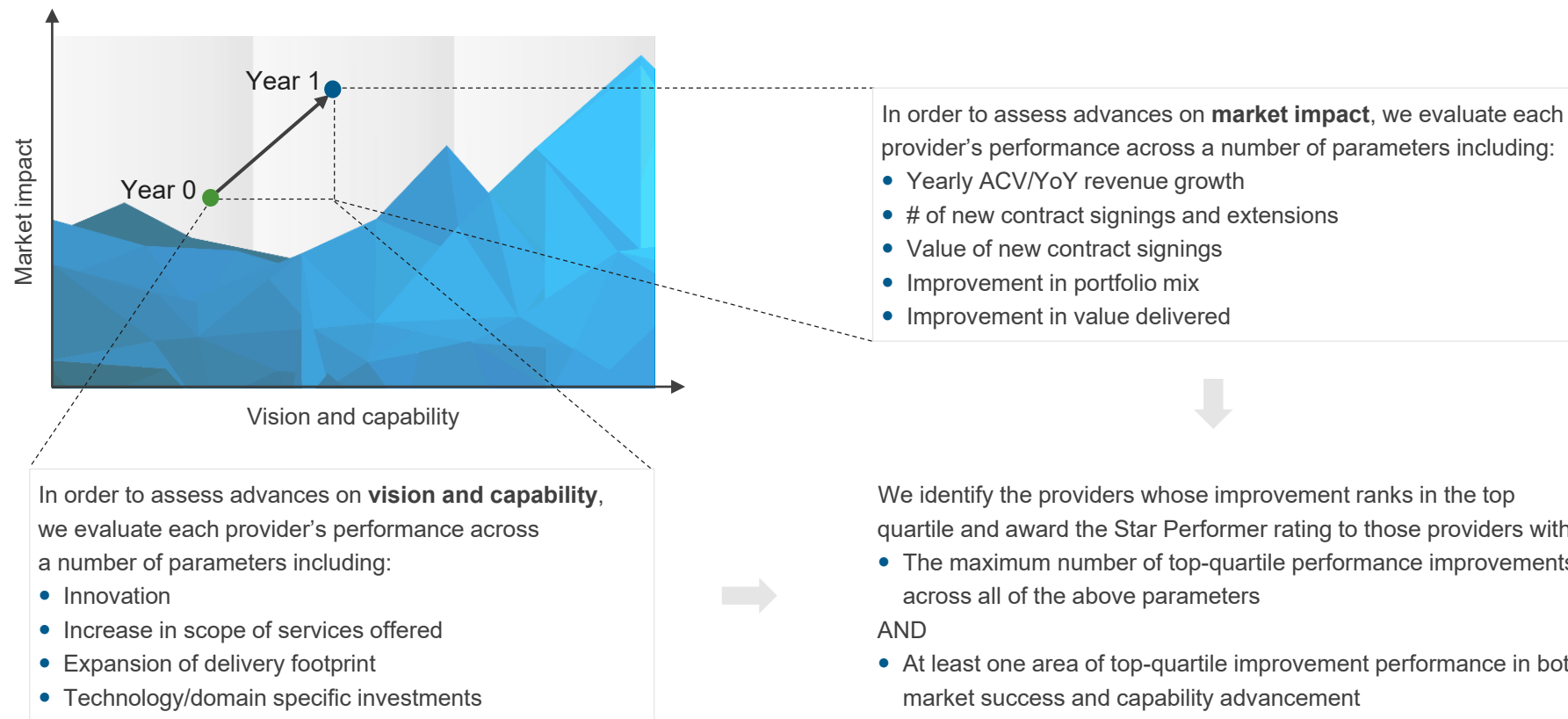
Services PEAK Matrix® evaluation dimensions



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.