



Everest Group Cybersecurity Services PEAK Matrix® Assessment 2024 – Europe

Focus on Accenture

October 2024



Introduction

Data security and governance laws in Europe are increasingly stringent and dynamic, especially as new technologies such as generative AI gain traction. The rise of digital transformation trends, coupled with regulations such as the AI Act with special provisions for gen AI, presents unique challenges for European enterprises. These businesses face region-specific cybersecurity needs due to Europe's diverse cultural, linguistic, and operational landscape, which demands tailored solutions from service providers.

Simultaneously, the rapid adoption of cloud computing, IoT, and remote work has significantly expanded the attack surface, heightening vulnerability to complex cyber threats such as data breaches and ransomware. To address these challenges, service providers are developing advanced cybersecurity solutions such as AI-driven threat detection, zero trust frameworks, SASE, and autonomous Security Operations Centers (SOCs). Additionally, they are investing in talent development and automation to bridge the skills gap. As the digital landscape continues to evolve, the focus on proactive and adaptive security measures is expected to drive ongoing growth in the cybersecurity sector.

In the research, we present an assessment and detailed profiles of 28 cybersecurity service providers from the European region, featured on the [Cybersecurity Services PEAK Matrix® Assessment 2024 – Europe](#). 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 28 leading cybersecurity service providers featured on the **Cybersecurity Services PEAK Matrix® Assessment PEAK Matrix 2024 – Europe**:

- **Leaders:** Accenture, Deloitte, Eviden, EY, HCLTech, IBM, NTT DATA, TCS, and Wipro
- **Major Contenders:** BT Group, Capgemini, Cognizant, Computacenter, DXC Technology, Fujitsu, Infosys, Kyndryl, LTIMindtree, Orange Cyberdefense, Sopra Steria, Tech Mahindra, Telefonica, and T-Systems
- **Aspirants:** CyberProof, Reply, Stefanini, Tietoenvy, and Yash Technologies

Scope of this report

Geography: Europe

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, Eviden, EY, HCLTech, IBM, NTT DATA, 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 that 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 the leading technology providers in the region along with localized delivery centers

Major Contenders

BT Group, Capgemini, Cognizant, Computacenter, DXC Technology, Fujitsu, Infosys, Kyndryl, LTIMindtree, Orange Cyberdefense, Sopra Steria, Tech Mahindra, Telefonica, and T-Systems

- 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 are focused on building cybersecurity service offerings with specialized resources, domain expertise, and competitive pricing

Aspirants

CyberProof, Reply, Stefanini, Tietoevry, and Yash Technologies

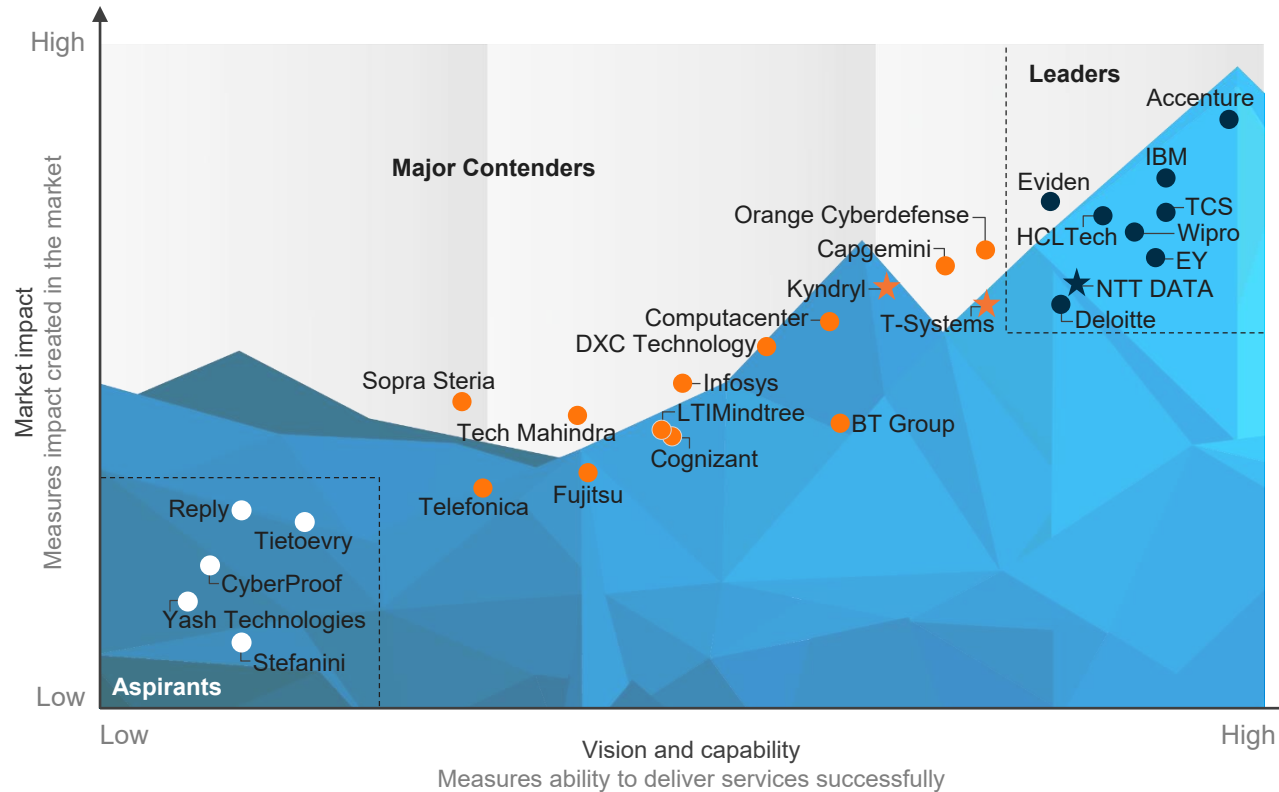
- The cybersecurity business of the Aspirants is still in its early stages and does not cater to the large or mega clients in the domain. These providers specialize in limited segments of cybersecurity, offering a narrow scope of services
- These providers are actively broadening their cybersecurity capabilities by leveraging strategic services, enhancing skills, and developing IP-driven solutions to better serve their clients
- These providers cater to enterprises across Europe by offering regional delivery footprints, making them the preferred choice for businesses seeking localized capabilities in specific segments of cybersecurity implementation

Everest Group PEAK Matrix®

Cybersecurity Services PEAK Matrix® Assessment 2024 – Europe | Accenture is positioned as a Leader

Everest Group Cybersecurity Services PEAK Matrix® Assessment 2024 – Europe¹

- Leaders
- Major Contenders
- Aspirants
- ☆ Star Performers



¹ Assessments for BT Group, Capgemini, Deloitte, Orange Cyberdefense, Sopra Steria, Telefonica, Tietoevry, and T-Systems 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 the buyers
Source: Everest Group (2024)

Accenture profile – Europe (page 1 of 8)

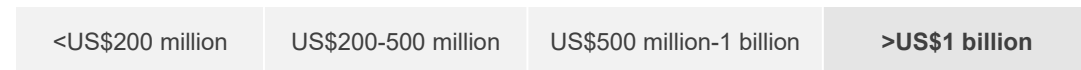
Overview

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 clients’ business, and position them for the future. Through highly differentiated security services, Accenture delivers 360° business value to clients, stakeholders, and the community. Accenture provides asset-led, industry-driven security solutions at speed and scale, leveraging onshore and offshore expertise, and innovative, collaborative approaches with clients. With security now the #1 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, and 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 – Europe (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

- UK & Ireland
- France & southern Europe
- Benelux
- Nordics
- DACH
- Others

Source: Everest Group (2024)

Accenture profile – Europe (page 2 of 8)

Case studies

[NOT EXHAUSTIVE]

CASE STUDY 1

Delivering next-generation security services

Client

A financial services company operating in Europe

Business challenge

The client identified a critical need for a strategic partner to address its cybersecurity challenges. Recognizing the importance of a strong security posture, it sought assistance in enhancing its cyber capabilities, adopting next-generation security operations, fostering innovation within its security function, and addressing the talent shortage hindering its progress toward a more mature security posture.

Solution

Accenture's cybersecurity solution provided a comprehensive range of services tailored to the bank's specific needs. By integrating with the bank's existing teams, processes, and tools, Accenture offered a tailored approach that included core managed security services, specified security services, and transformative security services. This comprehensive solution helped the bank to strengthen its security posture, protect its assets, and achieve the business objectives.

Impact

The transition was led by a skilled and experienced team, leveraging proven delivery methods to guide the bank through this change over a compressed timescale. Over 100 people were mobilized with 300+ hours of knowledge transfer and service design, for reviewing and accepting 100+ documents. Accenture enhanced the maturity of 30+ security services, optimizing cost models for improved business resiliency, cyber protection, and speed of detection and response.

Initiatives included:

- Enhanced security coverage
- Reduced false-positive alerting across a suite of security tools
- Improved identity and access management capabilities
- Enhanced Security Operations Center (SOC) capabilities

CASE STUDY 2

Developing dedicated initiatives in IT/OT security

Client

A multinational energy company in Europe with about 70 subsidiaries all over the world

Business challenge

The client needed a partner to address several critical cybersecurity challenges. These challenges included identifying and addressing technical vulnerabilities that could expose its IT/OT subsidiaries to cyberattacks, assessing the potential business impact of data breaches or disruptions to critical infrastructure, and staying informed about the evolving threat landscape to protect its valuable assets.

Solution

Accenture Security collaborated with the client's global cybersecurity department to provide comprehensive cybersecurity services for its IT/OT environment. The services included a cyber risk assessment based on international best practices, the development and implementation of remediation plans, the establishment of KPIs for cybersecurity monitoring, and the creation of a governance tool. This comprehensive approach helped the client identify and address vulnerabilities, improve its security posture, and ensure compliance with industry standards.

Impact

The activities, which were carried out in a worldwide and multicultural context, have allowed the client to:

- Increase the level of IT security on industrial sites
- Increase the level of cybersecurity awareness of employees and industrial suppliers
- Comply with sector regulations relating to the perimeter cybersecurity

Accenture profile – Europe (page 3 of 8)

Solutions

[REPRESENTATIVE LIST] [NOT EXHAUSTIVE]

Proprietary solutions / IP / Products

Solutions	Details
mySecurity Suite	mySecurity is a comprehensive cybersecurity suite offered by Accenture. It leverages generative AI and partner technologies to strengthen security across various areas, including cloud, identity, applications, platforms, and network operations.
Cyber Industry	It builds resilience and mitigates risk across each industry's value chain covering Comms, Media & Technology (CMT), products, health and public service, financial services, and resources. It embeds security to build cyber resilience and mitigate cyber risk across the 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"> It helps to 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 & Accelerators: mySecurity for Identity & Access Management (IAM); mySecurity for Applications; mySecurity for Cloud; mySecurity Diagnostic for AI & Data; mySecurity for Zero Trust, Network & SASE and Cybersecurity Mesh; and mySecurity for Enterprise Platform Security
Cyber Resilience	<ul style="list-style-type: none"> It builds pressure test defenses, understands emerging threats, and prepares and responds quickly to attacks. It includes offerings around cyber defense, cyber response, and cyber intelligence mySecurity Assets & Accelerators: mySecurity for Threat Detection & Response; mySecurity Portal for Managed Security Services; mySecurity for Cyber Defense; mySecurity for Cyber Intelligence; mySecurity for Cyber Response; and mySecurity Diagnostic for Cyber Resilience (CRD)
Cyber Strategy	<ul style="list-style-type: none"> It designs and operationalizes 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 (CaaS) mySecurity Assets & 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"> It helps protect operational reliability and integrity by securing industrial control systems and connected products at all stages of their lifecycle. mySecurity Assets & Accelerators: mySecurity for Operational Technology Security; Product Security Assessment; mySecurity for Threat Detection & Response; mySecurity Portal for Managed Security Services; and mySecurity for Cyber Response.

Accenture profile – Europe (page 4 of 8)

Investments, and recent activities

[REPRESENTATIVE LIST] [NOT EXHAUSTIVE]

Investments

Investments name	Details
Acquisition	Innotec Security: threat simulation, cyber risk assessment and security consulting, detection, response and incident management, cyber intelligence, infrastructure, and application security
Investments in start-ups	<p>Tenchi Security: third-party cyber risk management – SaaS platform connecting clients with their supply chains</p> <ul style="list-style-type: none"> • 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"> • Security Skill Up Program: a specialized skill up program open to all Accenture people in Europe interested in Cyber Careers; this program focuses on leading people from foundational to specialized security skills, including certifications • Cyber Hackademy 3.0 in Naples: promotes and builds security skills as one of the main pillars supporting society and economy, at the regional and national level • Security Pink Academy: a 24-week upskilling program for non-STEM females; as a result, 156+ non-STEM women were trained and hired since FY19
A US\$3 billion investment over three years in gen AI	<ul style="list-style-type: none"> • Accenture will double its 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 • The 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 – Europe (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 it is 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 that allow cybersecurity professionals to focus on more complex threats and 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 its 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: helps assess the threat from quantum, and define and modernize the security program, capabilities, and controls framework to enable secure post-quantum transformation • Crypto agility: deploys security controls and capabilities leveraging automation and crypto agility services where possible for continuous compliance • Post-quantum crypto: upgrade infrastructure and tools and begins installation for coming NIST post-quantum cryptography standards; enables 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 IAM in space, patch management in space, and enable 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 – Europe (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, Security Hub, etc.); Accenture is a launch partner for offerings such as the AWS Network Firewall, Accenture Flywheel and Continuous leveraging 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
Claroty	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	<ul style="list-style-type: none"> • Cloud: Accenture and Google Cloud are collaborating to provide businesses with the necessary expertise and tools to improve their security posture by developing robust security programs that ensure the protection of critical assets • Chronicle: Accenture's MxDR platform is integrated with Google Chronicle, allowing for enhanced threat detection, investigation, and response capabilities • Mandiant: Accenture collaborated with Mandiant to enhance cybersecurity capabilities for organizations by providing access to advanced threat intelligence and expertise
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 cybersecurity solution implementation

Accenture profile – Europe (page 7 of 8)

Partnerships

[REPRESENTATIVE LIST] [NOT EXHAUSTIVE]










Partnerships

Partners	Partnership type	Details
Okta	Technology partnership	Utilizing pre-configured use cases and rapid application onboarding to design and implement 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 IAM services; Accenture offers accelerators and IP including 20+ pre-configured use cases, an 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 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, VMWare.

Accenture profile – Europe (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 AI assisted SOC 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 suitable partner for enterprises seeking GRC services
- Enterprises seeking security consulting may find Accenture to be a suitable partner, as it offers IP-backed services that deliver value realization and RoI on cybersecurity investments
- Enterprises from the BFSI sector searching for risk assessment services will find Accenture to be a suitable provider with its IP Global Security Benchmark for Financial Services
- A few clients have praised Accenture for its blend of technical and business-centric solutions

Limitations

- Enterprises seeking extensive flexibility and customization may encounter limitations in Accenture’s offerings, as it primarily relies on providing on standardized solutions
- While clients have praised Accenture's technical capabilities, they expect better strategic-level assistance in its cybersecurity services
- Some clients have raised concerns about the need for simplification of threat reporting
- Clients have highlighted the limited visibility of Accenture’s platforms and IP and expect proactive showcasing of these internal solutions
- Enterprises must be cognizant of the fact that Accenture has limited presence in industries such as HLS and hi-tech compared to peers

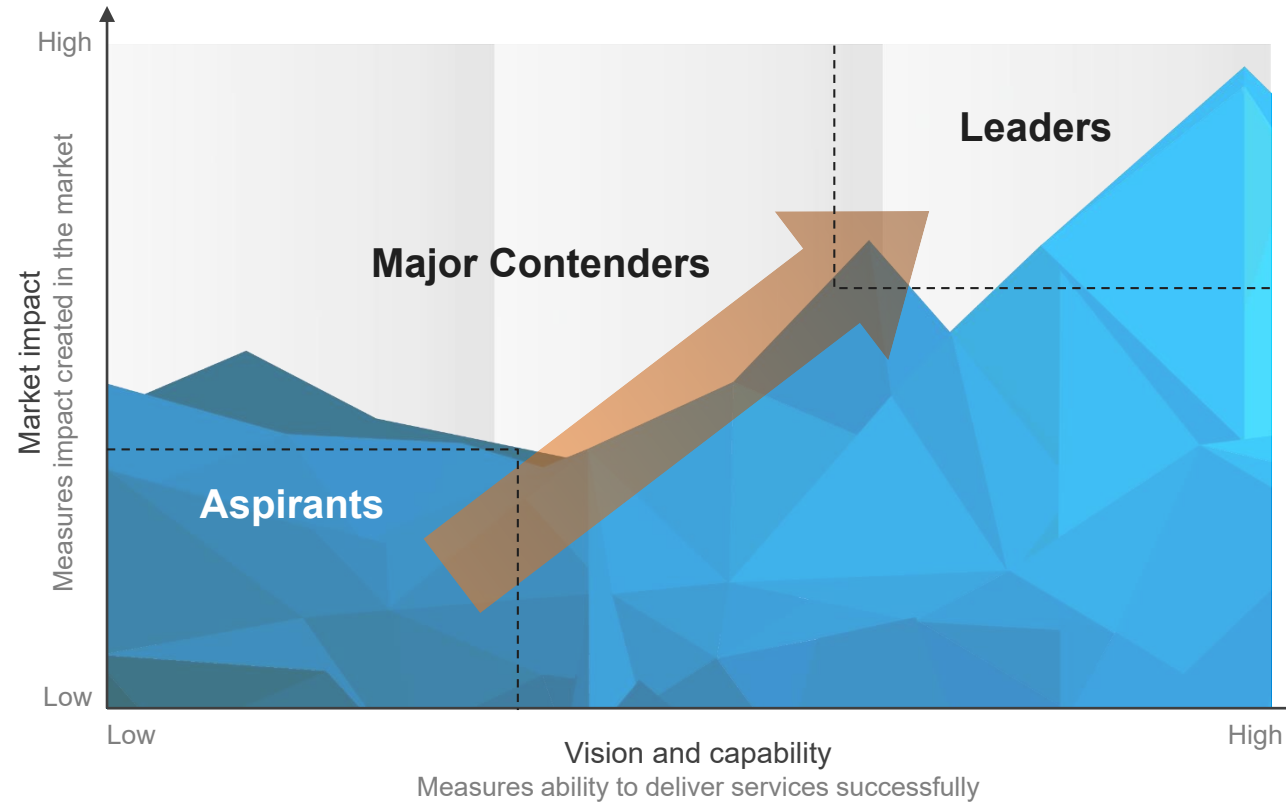
Appendix

PEAK Matrix® framework

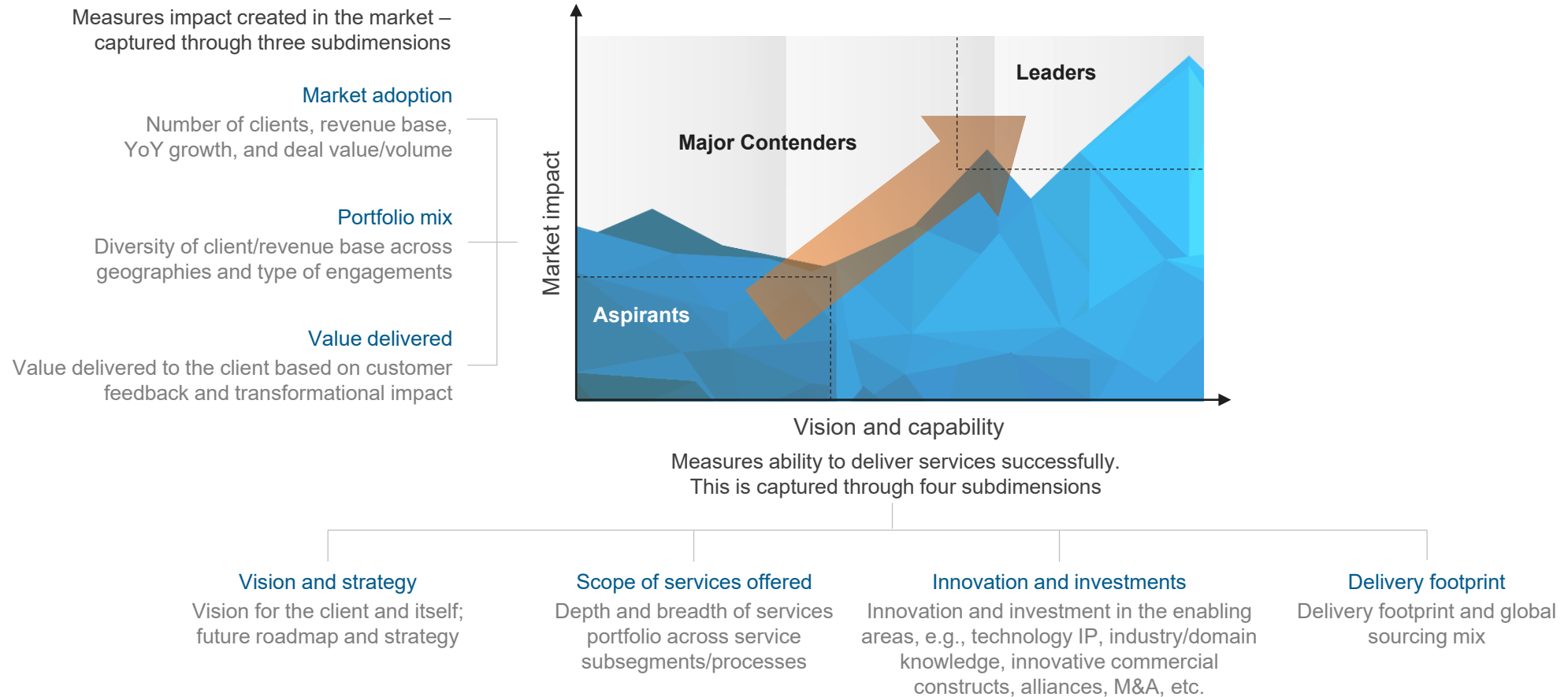
FAQs

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



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.