Everest Group®

Everest Group PEAK Matrix® for IT Security Service Provider 2022 – North America

Focus on HCL Technologies

August 2022

Everest Group
PEAK MATRIX®

Background of the research

Organizations are leveraging IT security services to improve their security posture and prepare for challenges such as ransomware attacks and business disruptions. The COVID-19 pandemic has further accelerated the adoption of security services, buttressed by enterprise challenges, in securing a remote workforce. Another important factor that has significantly contributed to the rise of IT security services is the shortage of expert cybersecurity talent and rising CAPEX and OPEX in maintaining in-house security teams, especially during the great resignation period. The US federal government too has taken a serious stance against cybercriminals and has been proactive in making laws and issuing executive orders covering a wide variety of security challenges ranging from OT security to data privacy laws such as CCPA and GDPR. All these factors combined have resulted in a major uptick in IT security services demand across the North American geography.

In this research, we present an assessment and detailed profiles of 27 IT service providers for the IT security capabilities in the North American region featured on the IT Security Services PEAK Matrix® Assessment 2022 – North America. The assessment is based on Everest Group's annual RFI process for the calendar year 2022, interactions with leading IT security service providers, client reference checks, and an ongoing analysis of the IT security services market.

The full report includes the profiles of the following 27 leading IT security service providers featured on the IT Security Services PEAK Matrix – North America:

- **Leaders:** Accenture, HCL Technologies, IBM, TCS, and Wipro
- **Major Contenders:** AT&T, Atos, Capgemini, Cognizant, Deloitte, DXC Technology, EY, Infosys, KPMG, Kyndryl, LTI, Microland, Mphasis, NTT DATA, PwC, Tech Mahindra, and Zensar
- **Aspirants:** GAVS Technologies, Happiest Minds, ITC Secure, Mindtree, and Yash Technologies

Scope of this report

Geography
North America

Providers
27

Services
IT Security Services

IT security services PEAK Matrix® – North America characteristics

Leaders:

Accenture, HCL Technologies, IBM, TCS, and Wipro

- Leaders have gained significant mindshare among enterprise clients due to the depth and breadth of their IT security services portfolio and on-ground presence in the North American geography. These players have a strong focus on next-generation security themes such as zero-trust, security analytics, OT security, security-embedded portfolio, Secure Access Service Edge (SASE), and Identity and Access Management (IAM)
- These providers have a highly balanced portfolio and continue to keep pace with market dynamics through continued investments in next-generation security solutions and services capability development (internal IP/tools, partnerships, etc.)

Major Contenders:

AT&T, Atos, Capgemini, Cognizant, Deloitte, DXC Technology, EY, Infosys, KPMG, Kyndryl, LTI, Microland, Mphasis, NTT DATA, PwC, Tech Mahindra, and Zensar

- These players have built meaningful capabilities to deliver IT security services; however, their service portfolios are not as balanced and comprehensive as those of Leaders (either in terms of coverage across IT security service segments, delivery mix, service type, or all)
- All these providers are making continued investments in developing internal IP and tools as well as expanding their service and technology partner ecosystem to plug their capability gaps, and are, thereby, positioning themselves as strong challengers to Leaders in this space
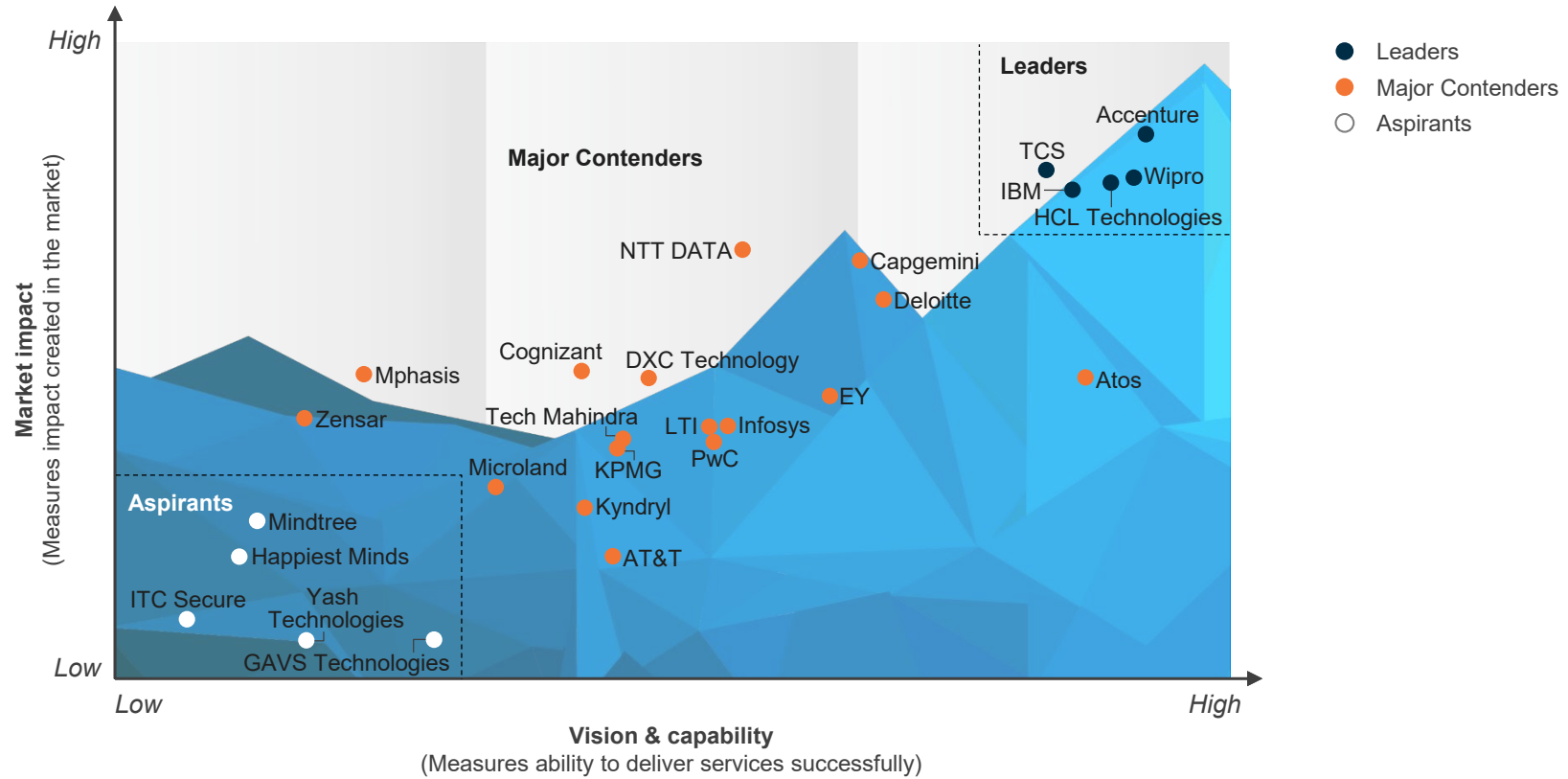
Aspirants:

GAVS Technologies, Happiest Minds, ITC Secure, Mindtree, and Yash Technologies

- The IT security services business of Aspirants is at a relatively early stage and is not a leading revenue generator for such players
- Nevertheless, these companies are making investments to build broader capabilities in the IT security services space to cater to buyers through service and technology partnerships as well as internal IP/tools – keeping them poised to be major challengers in the space

Everest Group PEAK Matrix®

IT Security Services PEAK Matrix® Assessment 2022 – North America | HCL Technologies positioned as Leader

Everest Group IT Security Services PEAK Matrix® Assessment 2022 – North America[1,2]

Legend:
- ● Leaders
- ● Major Contenders
- ○ Aspirants

Market impact (Measures impact created in the market) — vertical axis (Low to High)

Vision & capability (Measures ability to deliver services successfully) — horizontal axis (Low to High)

Leaders: Accenture, TCS, Wipro, IBM, HCL Technologies

Major Contenders: NTT DATA, Capgemini, Deloitte, Atos, Cognizant, DXC Technology, EY, Mphasis, Zensar, Tech Mahindra, LTI, Infosys, KPMG, PwC, Microland, Kyndryl, AT&T

Aspirants: Mindtree, Happiest Minds, ITC Secure, Yash Technologies, GAVS Technologies

1 Assessments for IBM, Capgemini, Deloitte, EY, KPMG, PwC, and AT&T based on Everest Group's proprietary Transaction Intelligence (TI) database, service provider public disclosures, and Everest Group's interactions with enterprise buyers
2 Analysis for LTI and Mindtree is based on capabilities before their merger

Source: Everest Group (2022)

HCL Technologies | IT security services – North America (page 1 of 10)
Everest Group assessment – Leader

Measure of capability: ⊙ Low ● High

Market impact				Vision & capability				
Market adoption	Portfolio mix	Value delivered	Overall	Vision and strategy	Scope of services offered	Innovation and investments	Delivery footprint	Overall
◕	◑	●	◕	●	◔	●	◔	◕

Strengths

- Enterprise buyers with global operations may find HCL to be a good fit because of its ability to deliver end-to-end security services at scale across multiple geographies

- In line with pandemic-led budget constraints, HCL has invested in bringing more automation to its security portfolio, building accelerators, and offering support for native cloud SecOps with wide integrations

- Enterprise buyers can benefit from HCL's investment in building a dedicated cybersecurity advisory practice – Fortius, that primarily provides security assessments and risk quantification services

- Enterprise buyers have appreciated HCL for its extensive security services such as XDR, SASE, zero-trust, converged IT OT, and DevSecOps

- Enterprises looking for embedded security in their IT services may find HCL to be a good fit because of HCL's secure-by-design set of offerings and IP

Limitations

- Clients have highlighted that HCL needs to invest more in vertical-specific dedicated Security Operation Centers (SOCs) such as automotive SOC and connected car SOC

- Clients have expressed concerns about HCL's lack of decisiveness and believe that HCL should focus on bringing in more innovation

- HCL needs to invest in expanding its on-ground presence for business proximity and better client intimacy

- Enterprise buyers from the public sector, manufacturing, and telecom, media & entertainment verticals must be wary as HCL lags peers in delivering verticalized security offerings for these sectors

Everest Group®

HCL Technologies | IT security services – North America (page 2 of 10)
Overview
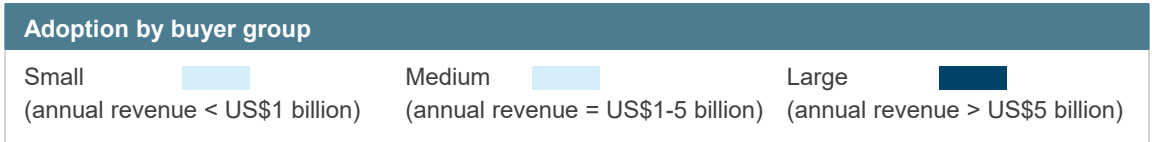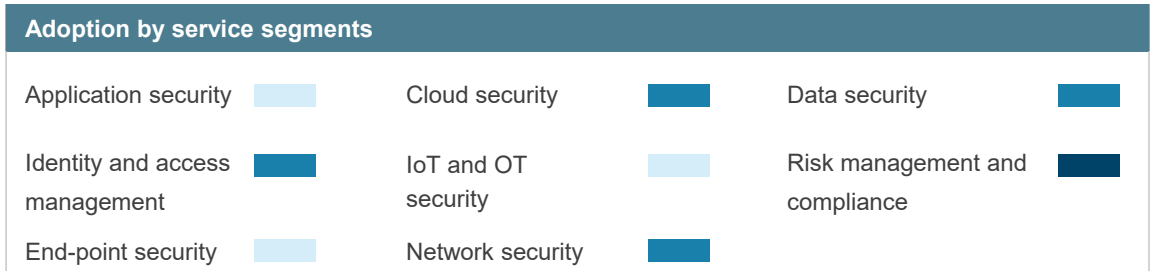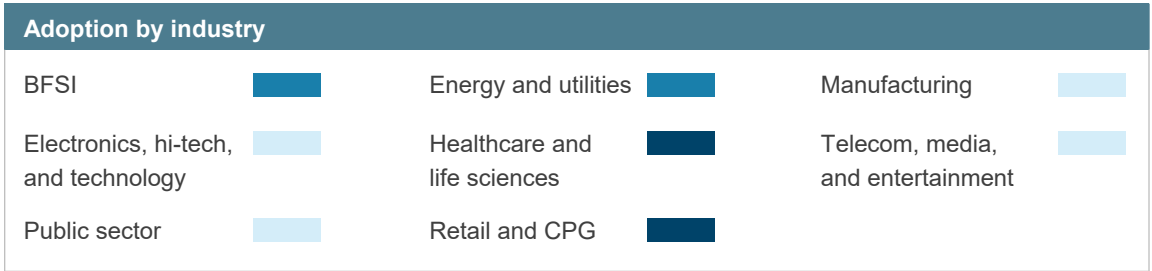
Low (<10%) Medium (10-20%) High (>20%)

Vision

HCL's vision for delivering IT security services is to be the trusted partner of enterprises in securing their digital enterprise journey through a dynamic risk and security apparatus that enables end-to-end cyber security capabilities in a single paradigm.

HCL delivers 360-degree dynamic security services ranging from strategy consulting & architecture, transformation & integration, and managed services with coverage across seven security solution domains in IT security services.

IT security services revenue (2021)

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

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 management and compliance	
End-point security		Network security			

Adoption by buyer group

Small (annual revenue < US$1 billion)		Medium (annual revenue = US$1-5 billion)		Large (annual revenue > US$5 billion)	

Adoption by country

Low (<15%) Medium (15-40%) High (>40%)

United States		Canada		Mexico	

Source: Everest Group (2022)

HCL Technologies | IT security services – North America (page 3 of 10)
Case studies

Case study 1	Threat intelligence for solving security assurance

Client: a Fortune 500 mining and fertilizer manufacturing a company headquartered in the US

Business challenge

The client needs to build a global delivery model to address regional challenges and boost cross-functional security assurance, including actionable operational KPIs and reporting. The transition strategy and deadlines must be consistent with the overall ITO solution and contain best practices for dealing with MTTD and MTTR risks.

Solution

To address geographic challenges, HCL employs the Sun Delivery model, which includes dedicated resources in the United States and Brazil, as well as best practice SLAs for monitoring and device management. They deliver frequent reporting and dashboard access for contextual threat intelligence. They have built SOC Automation and Ongoing Playbook Development, which are fueled by collaborative threat intelligence feeds, and they deliver a risk-free transfer utilizing their assets architecture.

Impact

- Reduced costs and improved operational efficiency by migrating all existing services to CSFC and implementing certified changes to aid
- Improved detection and repair of complex cyber-attacks by using Fusion MDR

Case study 2	A digital transformation for health care delivery system across the globe

Client: a US-based health network company

Business challenge

The client wanted to undertake digital transformation to improve its security posture, also it was running at a high cost.

Solution

HCL provides an Integrated Delivery Model and enterprise-wide security operations support. Through efficient GRC & BCP DR consulting and operations, they assist the client to build company resilience and comply with geo-specific regulations.

Impact

- Significant cost reductions while providing consumers with uninterrupted support and services
- A single dashboard view for the entire estate

HCL Technologies | IT security services – North America (page 4 of 10)
Solutions/IP/products

Proprietary solutions / IP / Products (representative list)	
Solution	**Details**
VERITY	HCL's VERITY is a comprehensive end-to-end platform that enables customers to reduce the risks of vulnerability exploitation by addressing the complete vulnerability lifecycle. Verity Framework provides coverage for any vulnerability throughout its lifespan and eventually strives to shorten the time it takes to mitigate by including risk, business effect, and asset criticality context to prioritize and focus on what matters most! One of the framework's important building pieces is the Vulnerability Management Office (VMO), which provides strategic and operational level oversight across the VM program to assure the program's efficacy and efficiency. VERITY provides inter-connected and centralized service deliverables for cloud and on-premise assets, policy compliance, application security, and offensive security.
MIDaaS	HCL MiDaaS is a comprehensive identity and access management system that includes the following features: • End-to-end managed service with HCL-owned licenses, operations, and expert services • It is a centralized service with entire monitoring fabric and IAM delivery under one roof, yet it is delivered internationally via onshore, offshore, and nearshore delivery models • It is based on DevOps and gives the client and HCL analysts real-time insights into the identity system
iAssure	• Centralized monitoring/alerting layer – application availability and performance monitoring • Monitoring/alerting delivered as part of HCL MTaaS (iAssure) • Standard Monitoring Parameters across IAM Applications
MyXylatics	MyXylatics provides customers with a dashboard view into the whole IAM ecosystem. • Standard reporting parameters across IAM applications and ITSM (incident & issue management) report supplied via MyXylatics • Dashboards for SLAs and KPIs • Reporting on application/tool use data (such as number of active identities managed, number of apps onboarded, connected vs disconnected, number of privileged accounts, and number of safes)
iAutomate	In some frequent use situations, RBA capabilities are powered by the iAutomate (DryIce) framework
iAssessment	• Current IAM status assessment based on industry standards and the IAM Strategy Roadmap • Model for application/device prioritization in IGA, PAM, SSO, and MFA • Based on CMM maturity levels and cloud adoption strategy, the IAM Maturity Model was developed

HCL Technologies | IT security services – North America (page 5 of 10)
Solutions/IP/products

Proprietary solutions / IP / Products (representative list)	
Solution	**Details**
iAccelerate	Monitoring automation framework helps to provide a centralized monitoring for the various IAM tools present in the customer's identity landscape through API based integrations with these tools.
CSaaS	HCL's Cloud Security as a Service (CSaaS) is an end-to-end service for customers that have a pure cloud/multi-cloud/hybrid cloud environment and is based on a borderless security foundation. The Borderless Security framework assists clients in implementing the appropriate protection policies to ensure complete security across networks, people, applications, and data located everywhere in the cloud, as well as secure application access from anywhere with a seamless user experience. HCL has a complete hybrid cloud security architecture in place that includes a detailed controls matrix that can be used to construct a robust security architecture that is aligned with the organization's security and business goals.
ASOC	HCL's Application Security Services portfolio is founded on products purchased from IBM Software, including Appscan, Big Fix, and others. From its cloud-hosted platform, HCL provides standardized application security services anywhere around the globe. HCL may also use the customer's investments in several products to safeguard their applications to offer MSS services.
BRiCS: Business Risk Intelligence and Compliance Solutions	• The BRiCS solution is an integrated, comprehensive approach to discovering, analyzing, and managing the dynamic interdependence of business and IT, as well as incorporating GRC disciplines into BAU tasks. Through a series of productive procedures, BRiCs effectively bridge the gap between the IT and business sides of enterprises. • The BRiCs framework includes 10 process domains that have been designed to serve industry specific verticals in terms of regulatory compliances, risks associated with Industry specific products, services, and business processes, repository of internal procedures & controls, audit procedures, role & responsibility matrices, and qualitative & quantitative mechanism to check & monitor the organizations' performance.
HCL RiCON Framework	• HCL provides BCP/DR services with its proprietary RiCON framework (risk-based continuity framework). HCL's RiCON is a one-of-a-kind service that handles each step of the BCP/DR life cycle with a focus on evolving business needs. It's intended to help with operational continuity, industry-specific regulatory compliance, and integrated IT risk management. • HCL's service offerings are intended to guarantee that business BCM requirements are risk-oriented and provide the company with a competitive advantage. Because most businesses have previously adopted BCM in some form or another, HCL's services are tailored to their individual needs and may either aid with any of their specific requirements or serve to establish the whole BCM framework as a greenfield project.

HCL Technologies | IT security services – North America (page 6 of 10)
Solutions/IP/products

Proprietary solutions / IP / Products (representative list)	
Solution	**Details**
HCL PrivacyOps Framework	• **Privacy readiness:** HCL Data Privacy Services' Privacy Readiness Program assists enterprises in measuring, evaluating, and analyzing their privacy posture in the light of developing data privacy standards
	• **PI modeling and mapping:** People and data mapping data graphs assist enterprises in understanding the context and presence of personal data across the company. This facilitates the efficient management and tracking of personal data through automation and artificial intelligence
	• **Data subject access rights (DSAR):** Hcl's regulatory-compliant DSAR service provides a one-stop solution for quickly satisfying the customer's data access rights
	• **Cookie consent and compliance:** Cookie consent and compliance management are now required by many data privacy rules. To fulfill all the legal requirements, HCL's cookie consent and compliance management solution aids companies in tracking consents and producing a real-time compliance dashboard
HCL SPADE (Security Posture Assessment for Dynamic Enterprises)	HCL SPADE is a platform that enables an enterprise-level assessment approach for assessing organizational security maturity levels across the IT infrastructure and application ecosystem. HCL SPADE is a comprehensive assessment methodology complying with industry best practices that cater to all security assessment demands of an organization's assets across the infrastructure and application ecosystem. It computes a SPADE score by doing a comprehensive and extensive security evaluation on architecture, configuration, content, and system.
AppScan	Its leveraged application vulnerability management and enabled companies to integrate security as a fundamental component of DevOps.
Grace Platform	Grace is HCL's Risk & Compliance Automation Dashboard, which offers customizable dashboards and assesses risks for clients across verticals, assisting them in launching their digital transformation journey while maintaining visibility on compliance and business risks.
HCL Fusion Platform	• HCL's proactive approach to Threat Detection and Response is made possible by the CSFC Fusion Platform. The tight integration of human experience, mature procedures, and machine intelligence enables CSFC security analysts to acquire total visibility, execute extensive cyber threat analysis, and respond quickly.
	• HCL monitors telemetry across the network, infra, hybrid cloud, and contemporary apps on-premises and in the cloud using its Fusion Platform.
	• HCL Fusion Platform provides Extensive Threat Visibility with unrivaled coverage, SaaS Scalability with built-in maturity, continuous threat detection with leading cyber intel, and incident containment in seconds through out-of-the-box system orchestration and standard playbook automation.
	• The HCL Fusion Platform also enables clients to reap the advantages of their existing SIEM investments, since many of them may now be integrated with the HCL Fusion Platform. Furthermore, by leveraging SOAR technology built on top of this platform, HCL's centralized workbench enables analysts to perform proactive threat hunts, automate enrichment, and accelerate reaction times through pre-defined bespoke playbooks.

HCL Technologies | IT security services – North America (page 7 of 10)
Solutions/IP/products

Proprietary solutions / IP / Products (representative list)	
Solution	**Details**
SecIntAI	HCL SecIntAI framework is a proactive threat mitigation product that uses big data analytics and artificial intelligence to prevent sophisticated attacks while detecting and responding to threats using global threat intelligence and contextual information. The following modules comprise the SecIntAI framework: • **Data collection and correlation:** Timely log collection and correlation from all sources • **Vulnerability and risk management:** Assessment of vulnerabilities, threat modeling, risk assessment, and prioritization • **Collaborative threat intelligence:** Integration of global threat intelligence and rule updates • **Security analytics:** Context enrichment via machine learning and derivation of actionable insights using advanced analytics • **Incident response:** AI-enhanced and automated incident response and forensic help
CRaaS (Cyber Resiliency as a service)	Cyber resilience necessitates careful preparation as well as the appropriate instruments. It is an iterative approach that guides recovery while keeping the company on high alert. As demand for this service grows across sectors, HCL has expanded its business resiliency and disaster recovery offering to include cyber recovery solutions. An operationally air-gapped cyber vault for storing and retrieving vital data is a key component of the system.
DIG-I-FORT	It is a cutting-edge framework created in-house that leverages next-generation technologies for infrastructure protection and ecosystem assurance.
3PAS	A holistic framework for third-party risk management solutions and services, which helps organizations to achieve end-to-end supply chain security compliance.
360 Degree SECUREOT	An in-house framework to safeguard enterprise-critical infrastructure – aids in the assessment, stratification, design, and redesign of industrial security measures through a solid strategy.
BigFix	This platform is being used to provide unified vulnerability management services, which include vulnerability detection and risk-based prioritized patching.

HCL Technologies | IT security services – North America (page 8 of 10)
Partnerships

Partner	Partnership type	Details
Armis, Claroty, Fortinet, Tenable, Microsoft, CheckPoint, and Cisco	IoT and OT security technology	To strengthen its OT security services portfolio, it has partnered with leading players in this space to develop joint offerings and strategic GTMs around ICS security solutions. Partnerships in this space have enabled HCL to cater to the highly verticalized use case demands of our clients.
Symantec, Tenable Inc., Terranova, Ironscales, Qualys, Inc, Risksense, Cylance Inc., Tanium, Inc., Proofpoint, Microsoft, and Carbon Black	End-point security Technology	HCL has strategic partnerships in this space and even a customer for these OEMs who get firsthand information of all the latest updates, product releases, information about new product launches, etc., that it leverage to serve the clients. The partnership focus areas include • Hybrid cloud security • Cloud workload protection • Digital consulting and transformation • Network security and access control • Endpoint security and proactive threat hunting • Comprehensive visibility, threat detection, and response
RSA, Stealthbits Technologies, Sailpoint, Inc, One Trust, BigID, CyberArk, Okta, Sailpoint, Saviynt, ForgeRock, and Microsoft	Identity and access management technology	HCL has developed strategic partnerships within the Identity spectrum of vendors to develop and deliver services around securing the hybrid identity as part of our wider identity and access management service portfolio. HCL has continuous engagements along with these vendors to enhance our specific service offering and develop joint GTMs.
ProcessUnity, Security Scorecard, Ascent Business Technology, Inc., Digital Shadows, Anamoli, MetricStream, ServiceNow, Securiti.ai, Security Scorecard	Risk management and compliance technology	Within the governance risk & compliance practice, HCL partners with the best-of-breed players to cater to the increasing customer challenges across supply chain risks, third party risk assessments, regulatory compliance, BCP/DR, and much more catering to industry-specific use cases.

Partnerships (representative list)

HCL Technologies | IT security services – North America (page 9 of 10)
Partnerships

Partnerships (representative list)		
Partner	**Partnership type**	**Details**
Securiti.AI, Mentis, Varonis, Metric Stream, Thale, Forcepoint, IBM, Microsoft, Microfocus, Fortanix, and Hashicorp	Data security technology	HCL has leveraged our strategic partnerships to jointly develop and take to market-focused service offerings in the area of data security. Key areas of joint development include: ● Database activity monitoring ● Data discovery-as-a-service ● Cryptography-as-a-service ● Data governance ● Database & privacy assessment, etc.

HCL Technologies | IT security services – North America (page 10 of 10)
## Investments, and recent activities

Investments (representative list)	
Investment name	**Details**
Acquisitions	HCL acquired DWS Limited and a chosen suite of IBM security products. Most Broadcom's symantec enterprise consulting staff has been transferred to HCL as part of the cooperation. This comprises endpoint security, online security services, cloud security, and data loss prevention capabilities. This allows HCL to establish a solid security consulting practice.
Talent	• HCL has established cyber security as a topic in Shiv Nadar University's Engineering curriculum and had such engineers hired into the cyber security teams • HCL has also collaborated with IIT Kanpur. HCL will partner with C3iHub, a specialist cybersecurity research center at IITK, to strengthen its expertise in the field of cybersecurity. As one of the initial areas of focus, HCL and IITK will offer real-world industry experience to carry out cooperative efforts and research to establish a security framework and solutions for cybersecurity concerns in present and future operating technologies • HCL has teamed with Microsoft, AWS, Azure, and CISCO to begin on a path of certification upskilling. Such certification programs have been created by our dedicated BU teams • HCL has an in-house learning management system with co-produced and in-house developed material on several securities and non-securities issues, as well as learning pathways for personas ranging from freshers to senior executives • Developing an ELITE employee program to address cybersecurity human resource requirements by successfully upskilling and laterally shifting individuals to delve into new areas of interest and offering considerable growth potential not just locally but worldwide
Others	• Advancement in managed SASE and managed SD-WAN solution offerings, including thorough IT architecture consulting, solution implementation, and managed services to manage and administer zero trust-based architectures • Extensive marketing and awareness campaigns, including tweet chats, LinkedIn Live sessions, blog and whitepaper publications, digital campaigns, executive roundtables, sponsorships, and so on, with the goal of raising awareness of the importance of securing everything and how HCL can assist in achieving the client's security visions • CSFC Development to Vietnam — As part of the worldwide expansion plan, HCL has begun investing in the establishment of a new Cyber Security Fusion Centre in Vietnam

Appendix

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

Everest Group PEAK Matrix
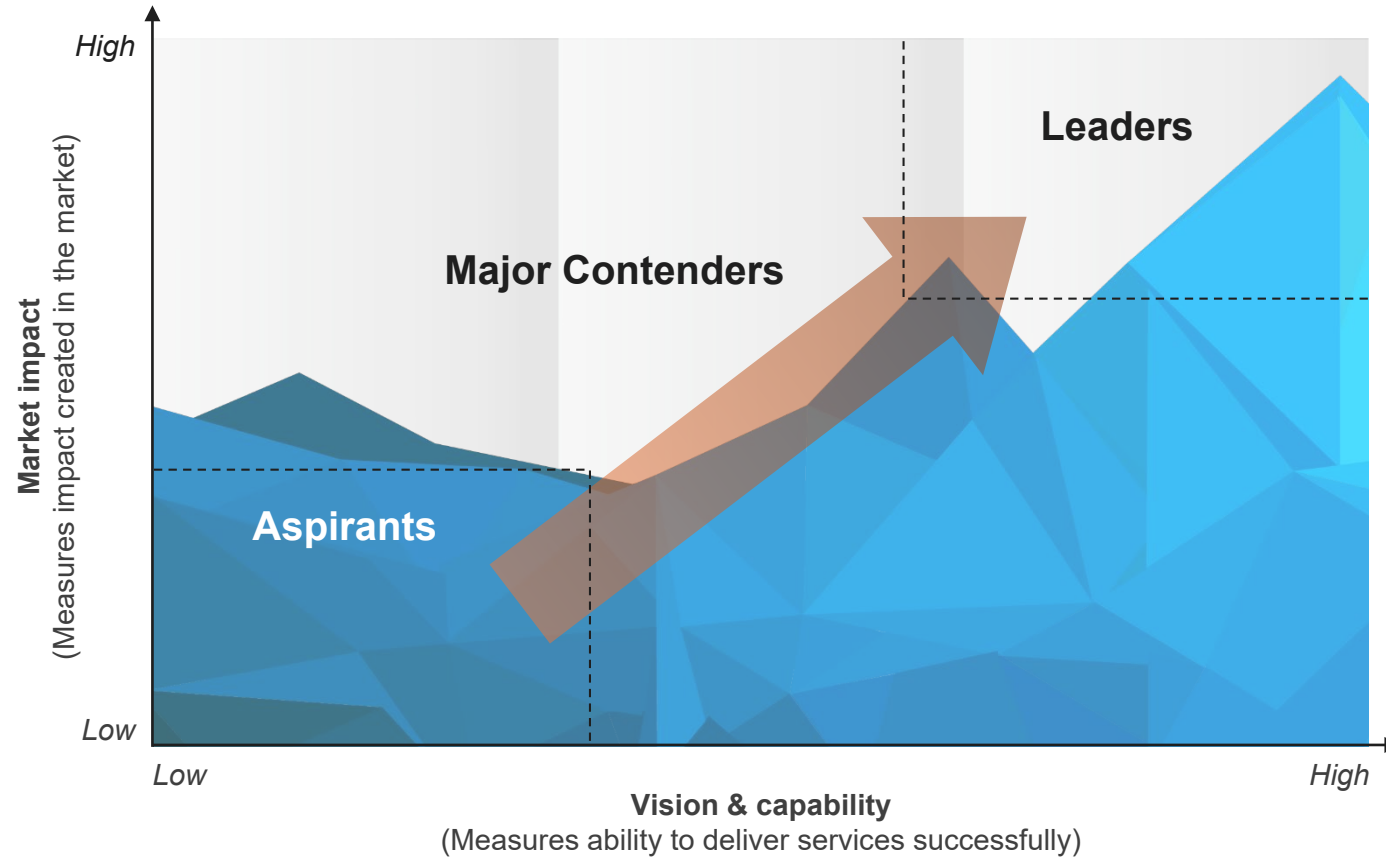
Services PEAK Matrix® evaluation dimensions

Measures impact created in the market – captured through three subdimensions

Market adoption

Number of clients, revenue base, YoY growth, and deal value/volume

Portfolio mix

Diversity of client/revenue base across geographies and type of engagements

Value delivered

Value delivered to the client based on customer feedback and transformational impact

Market impact

Leaders

Major Contenders

Aspirants

Vision & capability
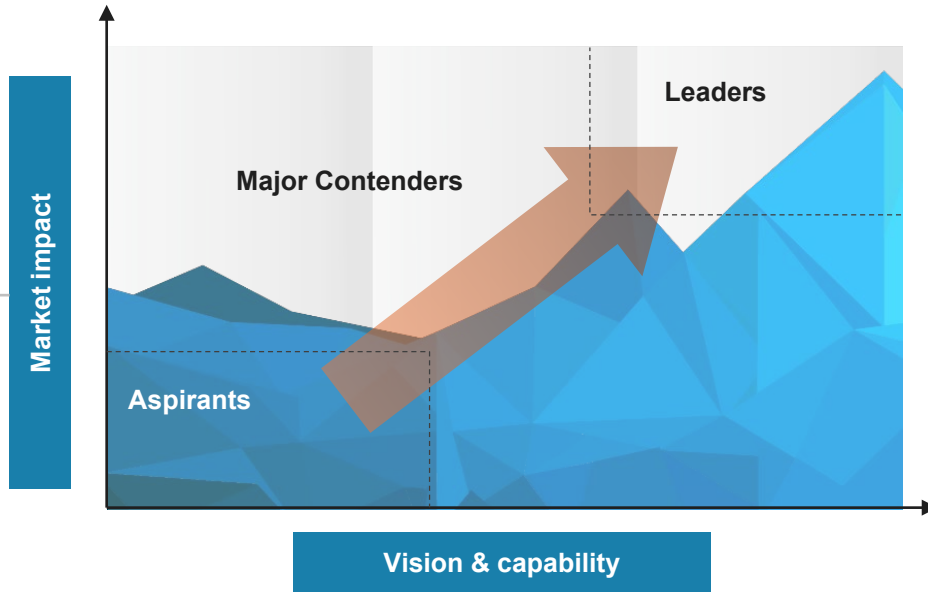
Measures ability to deliver services successfully. This is captured through four subdimensions

Vision and strategy

Vision for the client and itself; future roadmap and strategy

Scope of services offered

Depth and breadth of services portfolio across service subsegments/processes

Innovation and investments

Innovation and investment in the enabling areas, e.g., technology IP, industry/domain knowledge, innovative commercial constructs, alliances, M&A, etc.

Delivery footprint

Delivery footprint and global sourcing mix

FAQs

Does the PEAK Matrix® assessment incorporate any subjective criteria?
Everest Group's PEAK Matrix assessment adopts an unbiased and fact-based approach (leveraging provider / technology vendor RFIs and Everest Group's proprietary databases containing providers' deals and operational capability information). In addition, these results are validated / fine-tuned based on our market experience, buyer interaction, and provider/vendor briefings

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

What other aspects of PEAK Matrix assessment are relevant to buyers and providers besides the "PEAK Matrix position"?
A PEAK Matrix position is only one aspect of Everest Group's overall assessment. In addition to assigning a "Leader", "Major Contender," or "Aspirant" title, Everest Group highlights the distinctive capabilities and unique attributes of all the PEAK Matrix providers assessed in its report. The detailed metric-level assessment and associated commentary is helpful for buyers in selecting particular providers/vendors for their specific requirements. It also helps providers/vendors showcase their strengths in specific areas

What are the incentives for buyers and providers to participate/provide input to PEAK Matrix research?
- Participation incentives for buyers include a summary of key findings from the PEAK Matrix assessment
- Participation incentives for providers/vendors include adequate representation and recognition of their capabilities/success in the market place, and a copy of their own "profile" that is published by Everest Group as part of the "compendium of PEAK Matrix providers" profiles

What is the process for a provider / technology vendor to leverage their PEAK Matrix positioning and/or "Star Performer" status ?
- Providers/vendors can use their PEAK Matrix positioning or "Star Performer" rating in multiple ways including:
  – Issue a press release declaring their positioning. See citation policies
  – Customized PEAK Matrix profile for circulation (with clients, prospects, etc.)
  – Quotes from Everest Group analysts could be disseminated to the media
  – Leverage PEAK Matrix 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 the designated POC at Everest Group.

Does the PEAK Matrix evaluation criteria change over a period of time?
PEAK Matrix assessments are designed to serve present and future needs of the enterprises. 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 as well as serve the future expectations of enterprises

Everest Group®

With you on the journey

Everest Group is a research firm focused on strategic IT, business services, engineering services, and sourcing. Our research also covers the technologies that power those processes and functions and the related talent trends and strategies. Our clients include leading global companies, service and technology providers, and investors. Clients use our services to guide their journeys to maximize operational and financial performance, transform experiences, and realize high-impact business outcomes. Details and in-depth content are available at **www.everestgrp.com**.

Stay connected

Website
everestgrp.com

Social Media

🐦 @EverestGroup

in @Everest Group

f @Everest Group

▶ @Everest Group

Blog
everestgrp.com/blog

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
+1-647-557-3475