Cybersecurity Services PEAK Matrix® Assessment 2024 – North America

September 2024

PEAK MATRIX®

Cybersecurity

Everest Group®

Our research offerings

This report is included in the following research program(s):
Cybersecurity

- Advanced SciTech
- Amazon Web Services (AWS)
- Application Services
- Artificial Intelligence (AI)
- Asset and Wealth Management
- Banking and Financial Services Business Process
- Banking and Financial Services Information Technology
- Catalyst™
- Clinical Development Technology
- Cloud and Infrastructure
- Contingent Staffing
- Contingent Workforce Management
- Customer Experience Management Services
- CX Excellence
- CXM Technology
- Cybersecurity
- Cyber Threat Detection and Response
- Data and Analytics
- Digital Adoption Platforms
- Digital Services
- Digital Workplace
- Employee Experience Management (EXM) Platforms
- Employer of Record (EOR)
- Engineering Research and Development
- Enterprise Platform Services
- Exponential Technologies
- Finance and Accounting
- Financial Crime and Compliance
- Financial Services Technology (FinTech)
- Forces & Foresight
- GBS Talent Excellence
- Global Business Services
- Google Cloud
- HealthTech
- Human Resources
- Insurance Business Process
- Insurance Information Technology
- Insurance Technology (InsurTech)
- Insurance Third-Party Administration (TPA) Services
- Intelligent Document Processing
- Interactive Experience (IX) Services
- IT Services Excellence
- IT Talent Excellence
- Life Sciences Business Process
- Life Sciences Commercial Technologies
- Life Sciences Information Technology
- Locations Insider™
- Marketing Services
- Market Vista™
- Microsoft Azure
- Microsoft Business Application Services
- Modern Application Development (MAD)
- Mortgage Operations
- Multi-country Payroll
- Network Services and 5G
- Oracle Services
- Outsourcing Excellence
- Payer and Provider Business Process
- Payer and Provider Information Technology
- Price Genius – AMS Solution and Pricing Tool
- Pricing Analytics as a Service
- Process Intelligence
- Process Orchestration
- Procurement and Supply Chain
- Recruitment
- Retail and CPG
- Retirement Technologies
- Revenue Cycle Management
- Rewards and Recognition
- SAP Services
- Service Optimization Technologies
- Software Product Engineering Services
- Supply Chain Management (SCM) Services
- Sustainability Technology and Services
- Talent Genius™
- Technology Skills and Talent
- Trust and Safety
- Value and Quality Assurance (VQA)

If you want to learn whether your organization has a membership agreement or request information on pricing and membership options, please contact us at info@everestgrp.com

Learn more about
our custom research capabilities

Benchmarking

Contract assessment

Peer analysis

Market intelligence

Tracking: providers, locations, risk, technologies

Locations: costs, skills, sustainability, portfolios

Contents

For more information on this and other research published by Everest Group, please contact us:

Kumar Avijit, Vice President
Shivraj Borade, Senior Analyst
Arjun Chauhan, Senior Analyst
Prabhjyot Kaur, Senior Analyst
Shivam Naidu, Senior Analyst

Contents

Introduction and overview

Introduction

Summary

Background of research

Focus on research

Our research methodology is based on four pillars of strength to produce actionable and insightful research for the industry

01 Robust definitions and frameworks

Function-specific pyramid, Total Value Equation (TVE), PEAK Matrix®, and market maturity

02 Primary sources of information

Annual contractual and operational RFIs, provider briefings and buyer interviews, web-based surveys

03 Diverse set of market touchpoints

Ongoing interactions across key stakeholders, input from a mix of perspectives and interests

04 Fact-based research

Data-driven analysis with expert perspectives, trend-analysis across market adoption, contracting, and providers

Proprietary contractual database of over 350+ cybersecurity contracts (updated annually)

Year-round tracking of 80+ cybersecurity providers

Large repository of existing research in cybersecurity

Over 30 years of experience advising clients on strategic IT, business services, engineering services, and sourcing

Executive-level relationships with buyers, providers, technology providers, and industry associations

This report is based on key sources of proprietary information

- Proprietary contract-based database, which tracks the following elements of each contract:
  - Buyer details including size and signing region
  - Contract details including provider, contract type, TCV and ACV, provider FTEs, start and end dates, duration, and delivery locations
  - Scope details including share of individual buyer locations being served in each contract, Line of Business (LOB) served, and pricing model employed
- Proprietary provider database, which tracks the following elements of each provider:
  - Revenue and number of FTEs
  - Number of clients
  - FTE split by line of business
  - Revenue split by region
  - Location and size of delivery centers
  - Technology solutions developed
- Provider briefings
  - Vision and strategy
  - Annual performance and future outlook
  - Key strengths and improvement areas
  - Emerging areas of investment
- Buyer reference interviews, ongoing buyer surveys, and interactions
  - Drivers of and challenges to adopting services
  - Assessment of provider performance
  - Emerging priorities
  - Lessons learned and best practices

Providers assessed[1]

accenture · AT&T · AUJAS CYBERSECURITY · CGI · cognizant

CyberProof® A UST Company · Deloitte. · DXC TECHNOLOGY · <epam> · EY Building a better working world

EVIDEN · FUJITSU · GUIDEPOINT SECURITY · happiest minds · HARMAN

HCLTech · Infosys · innova SOLUTIONS · IBM · kyndryl

LTIMindtree · NTT Data · Orion Innovation · pwc · tcs TATA CONSULTANCY SERVICES

Tech Mahindra · verizon · wipro · World Wide Technology · YASH Technologies

[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
The source of all content is Everest Group unless otherwise specified
Confidentiality: Everest Group takes its confidentiality pledge very seriously. Any information we collect that is contract-specific will be presented only in an aggregated fashion

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. 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.

This 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

This report focuses on cybersecurity services and offers insights into the key cybersecurity services market trends

Consulting/assessment services

Policy and process consulting, vulnerability and risk assessment, audits, certification services, optimization and readiness assessment services, security architecture review, etc.

Design and implementation

Security architecture design and rearchitecting, security roadmap and strategy formulation, security implementation and integration services, etc.

Management and monitoring services

Asset management, continuous reporting and monitoring (including monitoring through SOCs), incident management/response, and SIEM/SOAR

Threat management

Threat detection, hunting, and response across end points, cloud, applications, IoT, OT, network, etc., threat intelligence, monitoring and reporting, digital forensics, log analysis, reduced MTTD and MTTR, etc.

Endpoint security

Host Intrusion Prevention Systems (HIPS), host-based firewalls, host-based Intrusion Detection Systems (IDS), virus and malware protection, device encryption, Mobile Device Management (MDM), etc.

Identity and access management

Authentication, authorization, access management, user provisioning, password management, PKI, Identity-as-a-Service (IaaS), privileged identity and access management, directory services, single sign-on, advanced identity services, monitoring and reporting, etc.

IoT and OT security

IoT device and data protection, asset discovery and intelligence, IoT threat intelligence, communication channel security, pre-embedded IDs and encryption, API access control, firmware update on IoT devices, OT device security, OT device monitoring etc.

Application security

Application security testing, application whitelisting, application self-protection, patching, application control, web application security (including firewalls), sandboxing, SAST/DAST, code hardening, API management, SSL offloading, etc.

Data security

Security services for structured and unstructured data: Data Loss Prevention (DLP), data encryption, protection and monitoring, database security, storage security, etc.

Cloud security

Security services specifically designed for securing and governing virtual workloads and hybrid IT environments: Cloud Access Security Broker (CASB), threat detection and response, identity management, cloud-native application and runtime security, cloud data security, cloud foundation security, etc.

Risk and vulnerability management and compliance

Governance, Risk, and Compliance (GRC) management, GRC-as-a-service, risk assessment as-a-service, compliance audits, compliance assurance, third-party risk management, vulnerability and patch management, risk quantification, security awareness training, etc.

Network security

Firewalls, Next-Generation Firewalls (NGFW), email/URL gateways, Network Intrusion Prevention Systems (NIPS), Distributed Denial-of-Service (DDoS) prevention and mitigation, Unified Threat Management (UTM), VPN, network control, Advanced Persistent Threat (APT) solutions, network access control, etc.

Disaster recovery

Automated point-in-time/granular recovery, disaster recovery orchestration, quick Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), data resiliency-as-a-service, disaster recovery-as-a-service, High Availability (HA) services, failover and failback automation, etc.

Cybersecurity services PEAK Matrix® characteristics

PEAK Matrix framework

Everest Group PEAK Matrix for Cybersecurity Services

Provider capability summary dashboard

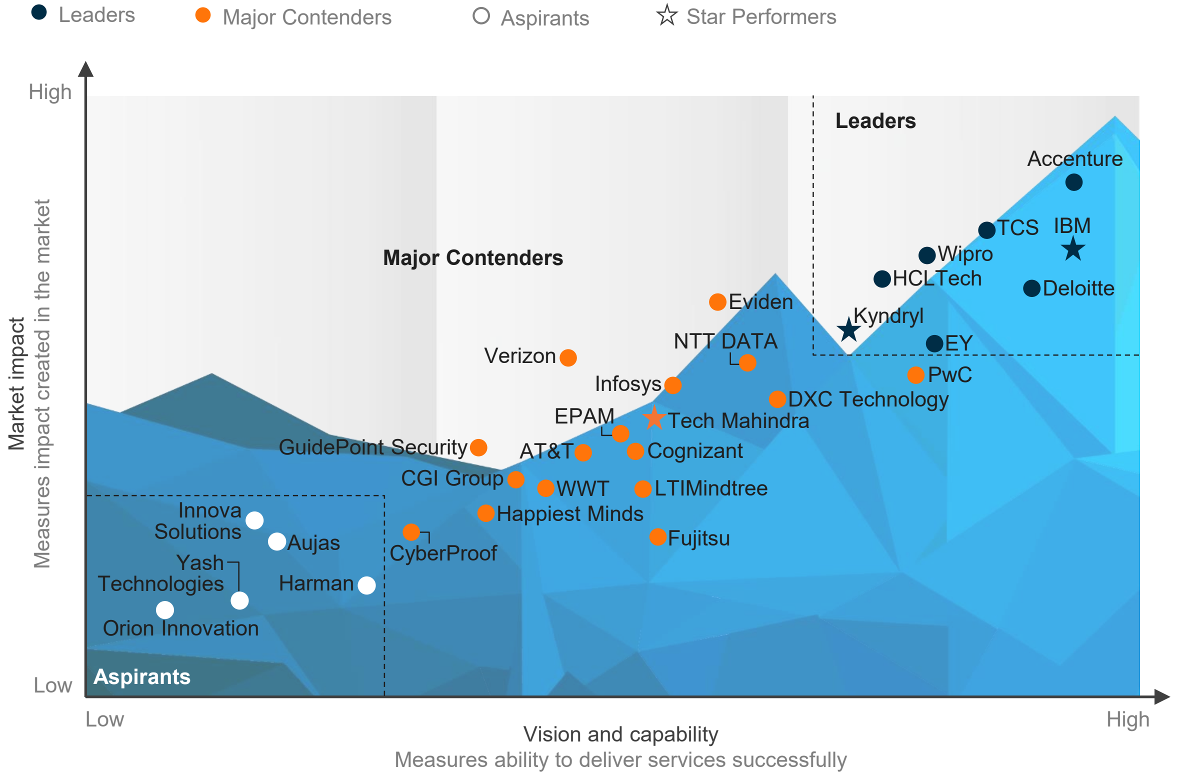
Characteristics of Leaders, Major Contenders, and Aspirants

Summary of key messages

Cybersecurity Services PEAK Matrix® Assessment 2024 – North America

- Everest Group classified 30 cybersecurity Service Providers (SPs) on Everest Group PEAK Matrix® into the three categories of Leaders, Major Contenders, and Aspirants
- The PEAK Matrix® is a framework to assess the market impact and vision and capability of service providers
- Based on Everest Group's comprehensive evaluation framework, the PEAK Matrix®, the 30 SPs evaluated are segmented into three categories (in alphabetical order within each category):
  - **Leaders:** Accenture, Deloitte, EY, IBM, Kyndryl, HCLTech, TCS, and Wipro
  - **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
  - **Aspirants:** Aujas, Harman, Innova Solutions, Orion Innovation, and Yash Technologies

Everest Group Cybersecurity Services PEAK Matrix® Assessment 2024 – North America[1]

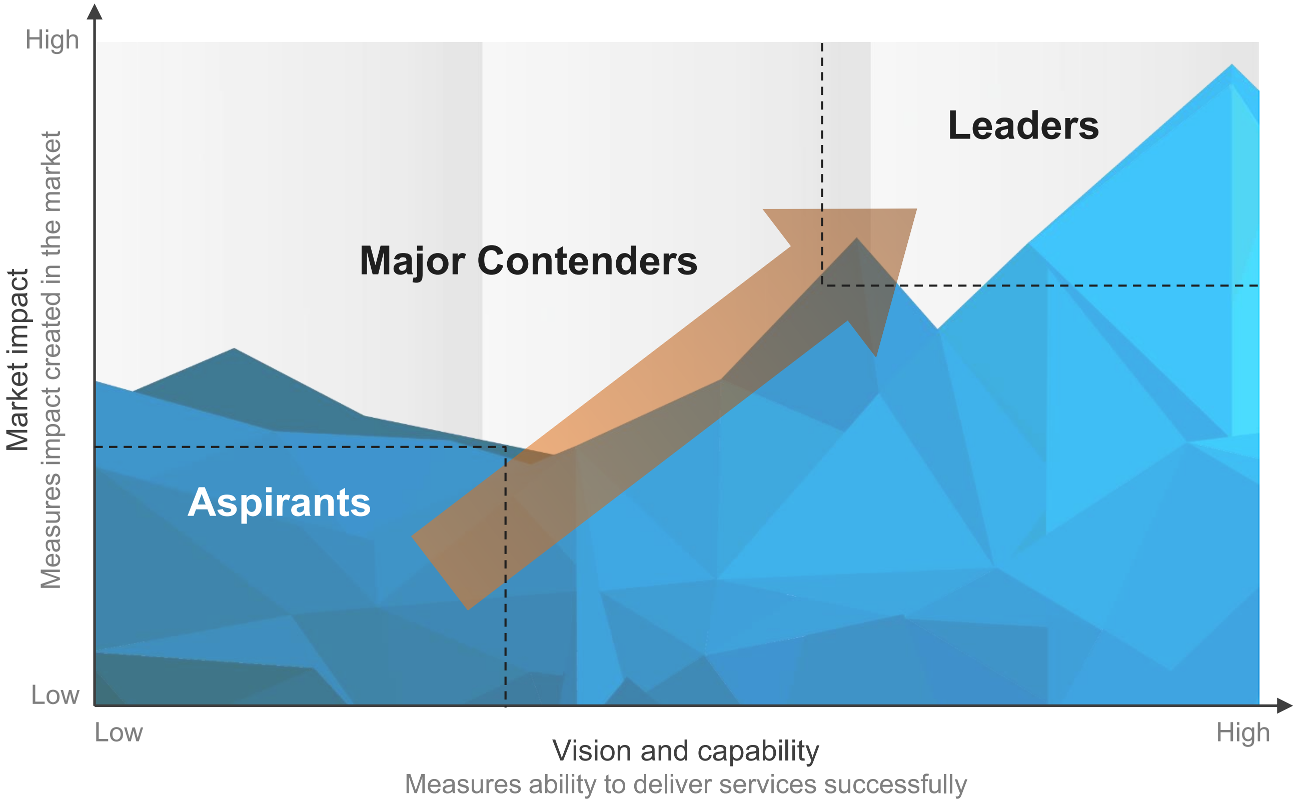


[1] Assessments for AT&T, CGI Group, Deloitte, PwC, and WWT excludes service provider inputs and are based on Everest Group's proprietary Transaction Intelligence (TI) database, provider public disclosures, and Everest Group's interactions with buyers

Source: Everest Group (2024)

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

Everest Group PEAK Matrix


High
Low
Market impact
Measures impact created in the market
Leaders
Major Contenders
Aspirants
Low
High
Vision and capability
Measures ability to deliver services successfully

Please click Everest Group PEAK Matrix® for more information

Services PEAK Matrix® evaluation dimensions

Measures impact created in the market – captured through three subdimensions

Market adoption

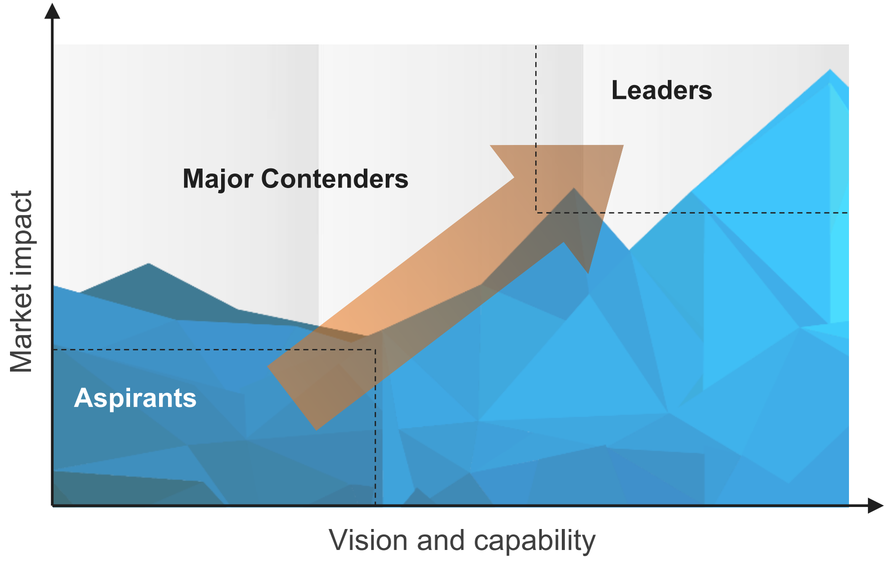
Number of clients, revenue base, YoY growth, and deal value/volume

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



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.

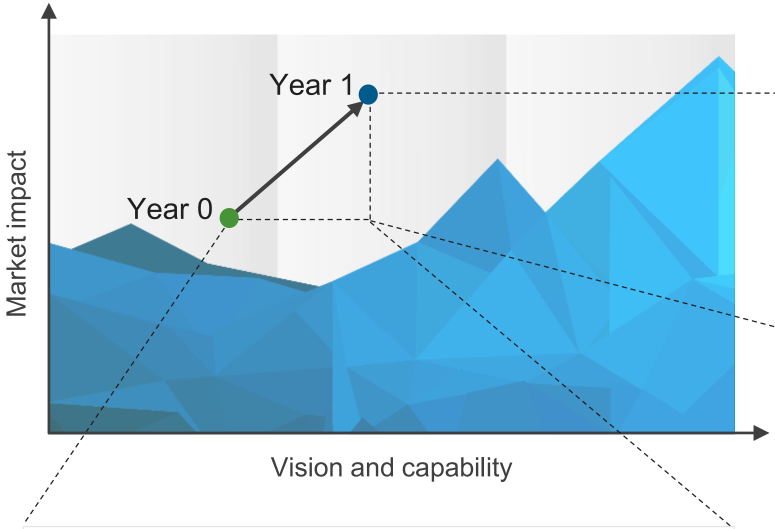
Delivery footprint

Delivery footprint and global sourcing mix

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



In order to assess advances on **market impact**, we evaluate each provider's performance across a number of parameters including:

- Yearly ACV/YoY revenue growth
- # of new contract signings and extensions
- Value of new contract signings
- Improvement in portfolio mix
- Improvement in value delivered

In order to assess advances on vision and capability, we evaluate each provider's performance across a number of parameters including:

- Innovation
- Increase in scope of services offered
- Expansion of delivery footprint
- Technology/domain specific investments

We identify the providers whose improvement ranks in the top quartile and award the Star Performer rating to those providers with:

- The maximum number of top-quartile performance improvements across all of the above parameters

AND

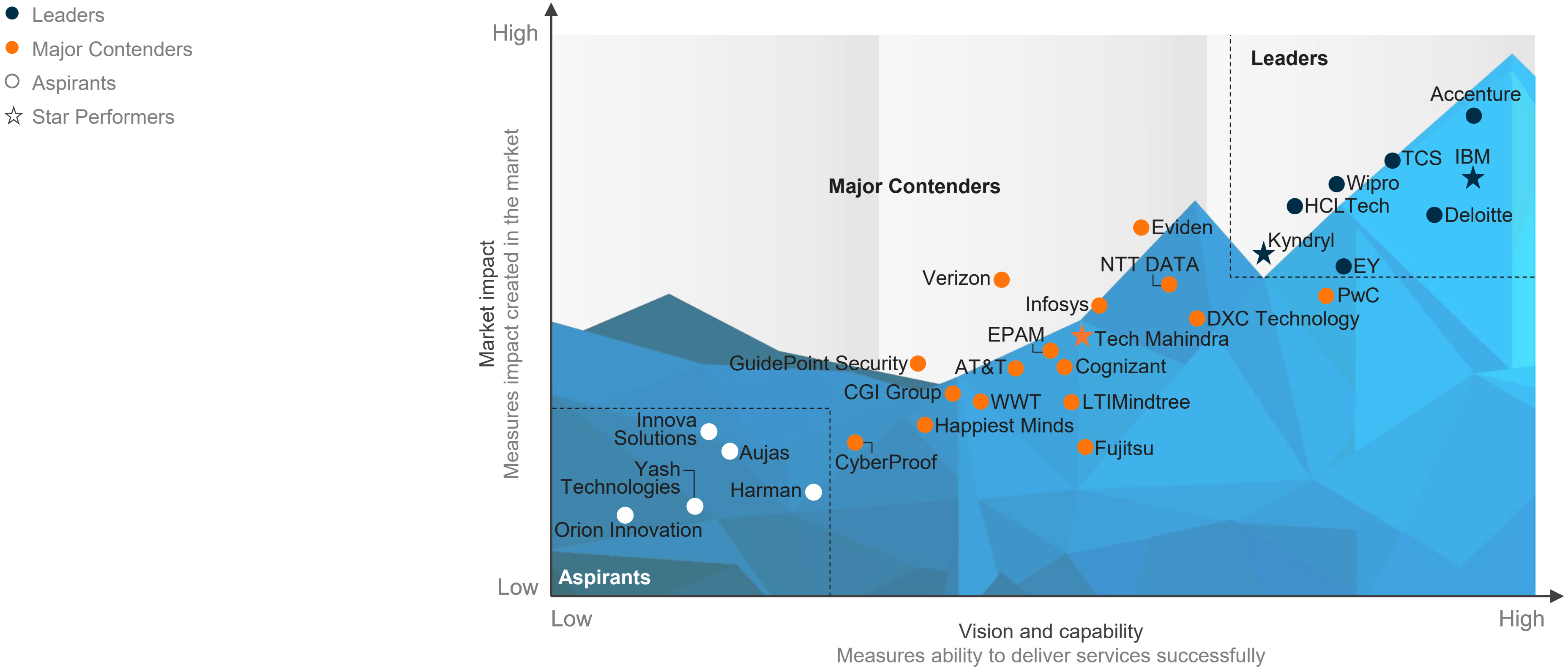
- At least one area of top-quartile improvement performance in both market success and capability advancement

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.

Everest Group PEAK Matrix®

Cybersecurity Services PEAK Matrix® Assessment 2024 – North America

Everest Group Cybersecurity Services PEAK Matrix® Assessment 2024 – North America[1]



[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)

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 has identified three providers as Star Performers in 2024

Cybersecurity services Star Performers	Distinguishing features of market impact in 2024	Distinguishing features of capability advances in 2024	Change in PEAK Matrix® positioning for Cybersecurity services
IBM	• Achieved significant client growth in cybersecurity services in 2024 • Improved its mega client market share in cybersecurity services in 2024	• Illustrated focus on enhancing gen AI-focused threat intelligence solutions • Enhanced its talent base to better serve clients across cybersecurity consulting services	Moved from **Major Contenders** to **Leaders**
Kyndryl	• Achieved significant YoY growth in cybersecurity services in 2024 • Improved its client market share in managed security services in 2024	• Improved its focus enhancing its partnership ecosystems • Demonstrated increased focus toward zero-trust implementation	Moved from **Major Contenders** to **Leaders**
Tech Mahindra	• Illustrated improved client feedback in cybersecurity services in 2024 • Experienced significant client growth 2024	• Demonstrated depth in vision and a promising roadmap for its cybersecurity services • Enhanced its commercial and engagement models to be better serve clients	Strengthened its **Major Contenders** positioning

Summary dashboard | market impact and vision and capability assessment of providers for Cybersecurity services 2024

Leader

Providers	**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
Accenture	●	◕	●	●	●	◕	●	◕	●
Deloitte	●	◕	◑	◕	◕	◕	◕	●	◕
EY	◕	◕	◑	◕	◕	◕	◕	◕	◕
HCLTech	◑	◕	●	◕	◕	◑	◕	◕	◕
IBM	●	●	◕	◕	●	◕	●	●	●
Kyndryl	●	◕	◑	◕	◕	◕	◑	◕	◕
TCS	◕	◕	●	◕	●	◕	●	◑	◕
Wipro	◕	◕	●	◕	●	◑	●	◑	◕

Summary dashboard | market impact and vision and capability assessment of providers for Cybersecurity services 2024 (page 1 of 2)

Major Contenders

Measure of capability: ◔ Low ● High

	Market impact				Vision and capability				
Providers	Market adoption	Portfolio mix	Value delivered	Overall	Vision and strategy	Scope of services offered	Innovation and investments	Delivery footprint	Overall
AT&T	◑	◕	◕	◑	◑	◕	◑	◑	◑
CGI Group	◕	◕	◔	◑	◑	◑	◔	◕	◑
Cognizant	◑	◑	◕	◑	◑	◑	◑	●	◕
CyberProof	◕	◔	◔	◑	◔	◕	◑	◑	◑
DXC Technology	◑	◑	◕	◕	◕	◑	◕	◕	◕
EPAM	◔	◑	◕	◕	◑	◑	◕	◑	◕
Eviden	◕	●	◕	◕	◕	◕	◑	◑	◕
Fujitsu	◕	◑	◔	◑	◑	◕	◑	◕	◕
GuidePoint Security	◕	◕	◑	◑	◑	◑	◑	◑	◑

Summary dashboard | market impact and vision and capability assessment of providers for Cybersecurity services 2024 (page 2 of 2)

Major Contenders

Measure of capability: ◔ Low ● High

	Market impact				Vision and capability				
Providers	Market adoption	Portfolio mix	Value delivered	Overall	Vision and strategy	Scope of services offered	Innovation and investments	Delivery footprint	Overall
Happiest Minds	◔	◔	◑	◑	◑	◕	◑	◔	◑
Infosys	◑	◔	◕	◑	◕	◔	◕	◑	◑
LTIMindtree	◑	◑	◑	◑	◑	◔	◑	◕	◑
NTT DATA	◑	◕	◕	◑	◑	◑	◕	●	◑
PwC	◕	◕	◑	◑	◕	◕	◕	●	◕
Tech Mahindra	◑	◑	◑	◑	◑	◕	◑	◔	◑
Verizon	◑	●	◕	◕	◑	◕	◔	◔	◑
WWT	◑	◑	◑	◑	◔	◔	◕	◑	◑

Summary dashboard | market impact and vision and capability assessment of providers for Cybersecurity services 2024

Aspirants

Measure of capability: ◔ Low ● High

	Market impact				Vision and capability				
Providers	Market adoption	Portfolio mix	Value delivered	Overall	Vision and strategy	Scope of services offered	Innovation and investments	Delivery footprint	Overall
Aujas	◔	◔	◕	◑	◔	◔	◔	◑	◔
Harman	◑	◑	◔	◑	◔	◕	◔	◑	◑
Innova Solutions	◑	◔	◕	◑	◑	◔	◔	◑	◔
Orion Innovation	◔	◔	◑	◔	◔	◔	◔	◔	◔
YASH Technologies	◔	◔	◑	◔	◔	◑	◔	◑	◔

Enterprise sourcing considerations

Leaders

- Accenture
- Deloitte
- EY
- HCLTech
- IBM
- Kyndryl
- TCS
- Wipro

Accenture

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

Deloitte

Everest Group assessment – Leader

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises form the public sector may find Deloitte a relevant service provider as it has credible delivery proof points and a significant market share of federal and defense clients
- Enterprises seeking risk and governance capabilities may find Deloitte to be a pertinent choice with its automation-embedded Enterprises Governance Risk and Compliance (EGRC) platform
- Deloitte's business process-oriented IAM framework enables it to provide enterprises with cost-effective and flexible IAM services
- Enterprises searching for cloud security services can benefit from its industry-contextualized Cloud Security Management (CSM) platform
- Clients have appreciated Deloitte's credible delivery footprint with a robust mix of onshore, offshore, and nearshore delivery centers

Limitations

- Enterprises seeking platform-led, end-to-end cybersecurity services should carefully assess Deloitte as it lacks a unified platform for holistic cybersecurity
- Enterprises with budget constraints may not find Deloitte a relevant choice due to its premium pricing compared to peers
- A few clients have highlighted a communication gap between the strategic team and the technical team of Deloitte
- Small buyers need to be aware that Deloitte is more focused on midsized and large clients in cybersecurity services
- Enterprises seeking extensive flexibility and customization may encounter limitations in Deloitte's offerings, as it primarily relies on standardized solutions

EY

Everest Group assessment – Leader

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises seeking PAM services may find EY to be a relevant choice, with robust service offerings, backed by its dedicated practice of Privilege Access Research and Inventory System (PARIS)
- Enterprises can leverage EY’s innovative OT security offerings with zero trust and metaverse security capabilities, along with cybersecurity solutions for emerging IoT industries such as smart cities and smart factories
- Enterprises may benefit from EY’s dedicated offering of analytics for cyber resilience, providing requirement analysis, cost analysis, and utilization analysis
- EY’s Center of Excellence (CoE) for crisis simulation, with SOC-in-a-box-as-a-service, allows enterprises to implement offensive security measures
- Enterprises looking for innovative cybersecurity services may find EY to be a strong partner of choice due to its investments in gen AI and quantum security

Limitations

- Enterprise need to be wary of EY’s limited maturity on SASE services and its limited market mind share
- Clients have raised concerns of EY’s premium pricing for cybersecurity services
- Enterprises seeking service providers with extensive incident response capabilities for OT assets should be aware of EY’s limited capabilities in this domain
- Enterprises looking for platform-led, end-to-end cybersecurity services must be aware that EY lacks unified platform-led cybersecurity offerings
- Small enterprises should be aware of EY's focus on midsized and large clients that can impact their domain expertise

HCLTech

Everest Group assessment – Leader

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises searching for localized delivery may find HCLTech to be a suitable partner, with its significant satellite delivery centers optimizing resource cost
- HCLTech has invested in expanding its partnership ecosystem, enabling it to offer enhanced vendor-specific cybersecurity capabilities for faster time-to-value realization for end clients
- HCLTech is a suitable choice for enterprises seeking cybersecurity consulting services, offering a blend of technical and business-centric solutions such as M&A and transformation consulting, underpinned by its Cloud Smart platform
- Enterprises from HLS and retail and consumer packaged goods verticals may find HCLTech to be a suitable partner with industry-specific strategic initiatives such as the HLS Identity Cloud
- Clients have praised the technical depth and cross-skilled capabilities of HCLTech's cybersecurity practitioners

Limitations

- While HCLTech excels in threat analytics with its Fusion platform, it lags delivery proof points in governance and application security segments
- Few clients expect better synergy between HCLTech's network and cybersecurity teams during implementation of network security services
- Clients have highlighted that HCLTech can play a more proactive role in enterprise decision-making and go beyond the immediate scope of delivery
- Clients have raised concern on HCLTech's project management, noting with communication gap and misaligned resource allocation
- Enterprises from the public sector vertical must carefully assess HCLTech due to its limited delivery footprint in the region

IBM

Everest Group assessment – Leader and Star Performer

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprise searching for governance, risk, and compliance services may find IBM suitable with its robust frameworks backed by automation and monitoring
- IBM has invested in gen AI-backed threat intelligence services that are embedded with its X-Force platform, allowing it to provide efficient cybersecurity services
- Enterprises seeking faster time-to-value in cybersecurity services may find IBM pertinent because if its platforms and accelerators such IBM Garage and Threat Operations Optimizer (TOO)
- IBM may be a relevant choice for the enterprises seeking industry-specific cybersecurity consulting services owing to its industry-focused accelerators such as Security Platform Architecture Blueprint and Secure Intelligence Process Workflows
- Enterprises searching for global delivery capabilities of cybersecurity services may appreciate IBM’s onshore, offshore, and nearshore presence

Limitations

- Enterprises must be wary of IBM's limited enterprise mindshare in delivering cybersecurity design and implementation services
- Enterprises seeking cost-effective service providers should carefully evaluate IBM due to its premium pricing
- Some clients have highlighted that IBM needs to play a more significant role in internal discussions and be a part of decision-making with senior stakeholders
- A few clients have highlighted that IBM needs to invest more in training and certifications of its resources
- IBM lags collaboration with niche technology providers such as Wiz and Checkmarx to deliver specialized solutions across different cybersecurity segments

Kyndryl

Everest Group assessment – Leader and Star Performer

Measure of capability: ◔ Low ● High

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

Strengths

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

Limitations

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

TCS

Everest Group assessment – Leader

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises from the BFSI sector may find TCS pertinent, with its industry-contextualized offering and extensive delivery proof points in the vertical
- TCS has invested in GRC services with its BlueTick portal, with pre-built assessment templates allowing it to provide quick compliance assessments
- Enterprises seeking service providers with global delivery capabilities for cybersecurity services may find TCS relevant, as it offers high scalability and delivery flexibility through its 150+ delivery centers and 40+ SOCs across the globe
- Some clients have appreciated TCS owing to its ability to introduce newer ideas and innovative solutions, while staying cost competitive
- Clients have praised the TCS team for rapid adaptation to the client environment owing to its flexible services implementation

Limitations

- While TCS has invested in OT/IoT security, enterprises must carefully assess TCS as it lags its peers in credible delivery proof points
- Enterprises from the public sector should be wary of TCS' limited presence in the vertical
- Small buyers should be aware of TCS' higher focus on midsized and large clients for cybersecurity services
- Some clients have noted that TCS could benefit from stronger alignment between the delivery and technical teams
- Some clients have highlighted attrition as a major challenge for TCS and the expectation will be to maintain same level of quality, even in case of attrition

Wipro

Everest Group assessment – Leader

Measure of capability: ◔ Low ● High

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

Strengths

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

Limitations

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

Enterprise sourcing considerations

Major Contenders

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

AT&T

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises seeking managed security services may find AT&T pertinent with its dedicated Level Blue business with focus on threat detection and response and threat intelligence
- AT&T's extensive experience in network services has enabled it to build robust network security and SASE-as-a-service for enterprises
- Enterprises from BFSI and HLS sectors may find AT&T to be a suitable partner as it has vertical-specific specialized practitioners and credible delivery proof points
- AT&T's investments in upskilling with the ACT learning portal for cross-skill development allows it to provide cost-competitive pricing with efficient talent
- A few clients have lauded the synergy between the NOC and SOC teams in the implementation of network and security services

Limitations

- AT&T lags its peers in showcasing credible delivery proof points around IAM services such as PAM, CIAM, and identity-based zero trust
- Enterprises seeking quick time-to-value in cloud security services such as CSPM and CNAPP should carefully evaluate AT&T as it lags its peers in automation embedded configuration management and posture assessments
- Enterprises looking for a service provider with a strong partnership ecosystem should evaluate AT&T as it lags its peers in cybersecurity partnerships
- AT&T may not suit enterprises seeking end-to-end security due to its reliance on multiple point solutions and the lack of a unified platform
- Enterprises seeking pure-play security consulting services must be wary of AT&T's limited capabilities in consulting services in few security segments such as GRC, application security, and data security

CGI Group

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises looking for managed security services may find CGI Group to be a suitable partner with its intelligent SOC, threat hunting, and Advanced Threat Intelligence (ATI) and forensics' MDR modules
- Public sector enterprises may find CGI Group to be a relevant service provider as it has credible security services delivery proof points in this vertical
- Enterprises may benefit from CGI Group's GRC capabilities as it offers unified governance monitoring and management for converged IT and OT infrastructure
- Clients have lauded CGI Group's capabilities to deliver tailored security services, leveraging the existing client technology stack
- Clients from the BFSI sector have appreciated the industry knowledge of the CGI Group practitioners

Limitations

- Enterprises should cautiously evaluate CGI Group's capabilities and must be aware of its limited investment in building its own platform and reliance on third-party tools for security implementations
- Enterprises seeking gen AI security should be aware of CGI Group's limited investments in building gen AI security services portfolio
- Enterprises looking for service providers with application security engagements might not find CGI Group to be relevant because of its limited delivery proof points and solutions
- Clients have highlighted that CGI Group lags its peers in investments in co-innovative security services
- Some clients believe that CGI Group should invest more in expanding its security partnership ecosystem

Cognizant

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises may find Cognizant to be a partner of choice in IAM, with its co-innovative solutions such as Identity Governance-as-a-Service (IGaaS) and converged IAM with Microsoft and Saviynt
- Enterprises searching for strong pure-play managed services may find Cognizant pertinent with its significant number of automation-embedded SOCs
- Cognizant has invested significantly in the adoption of gen AI with its IP such as Neuro AI, which allows it to provide threat intelligence services to clients
- Cognizant has a robust mix of onshore, nearshore, and offshore delivery footprint allowing it to offer flexible delivery options to clients
- Enterprises from the HLS industry may find Cognizant to be a suitable partner with high emphasis in avenues such as security for IT/OT convergence
- Enterprises can benefit from its strong presence in North America and can leverage its regional SOCs

Limitations

- Enterprises should be wary of Cognizant's limited cyber resilience services as it lags mature resiliency frameworks and delivery proof points
- While Cognizant offers zero-trust services, it lags peers in terms of enterprise mindshare for SASE due to limited of investments
- While Cognizant offers the Cyber Threat Defense (CTD) platform for MDR services, enterprises seeking comprehensive platform-led security might find it less suitable as it lags its peers in delivery services from a single unified platform
- While Cognizant has high emphasis in IAM, it lags focus on other security segments such as cloud security and OT/IoT security compared to peers
- Enterprises from the public sector should carefully evaluate Cognizant's capabilities due to its limited delivery proof points in federal clients and limited enterprise mindshare in the vertical

CyberProof

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises seeking end-to-end cybersecurity and resilience may find CyberProof to be relevant due to its phased roadmap based on cybersecurity maturity of the enterprise
- CyberProof's blend of consulting, implementation, and managed security services for enterprises seeking OT security makes it a relevant choice
- Enterprises from the BFSI sector may find CyberProof to be relevant in providing cybersecurity services as it has demonstrated credible delivery proof points
- Enterprises seeking SIEM-specific offerings may find CyberProof to be a preferred choice due to its dedicated analytics-driven solutions such as Log Ingestion and Data Aggregation
- Clients have lauded CyberProof for its onshore and nearshore presence of SOC analysts

Limitations

- Enterprises seeking localized delivery might not prefer CyberProof, as it offers remote SOC services in North America
- Few clients have highlighted CyberProof's limited presence in HLS, retail, and public sector in North America
- Enterprises seeking cloud security services need to carefully assess CyberProof's capabilities as it has limited delivery proof points compared to peers
- Large enterprises seeking end-to-end cybersecurity services must closely evaluate CyberProof as it has limited cybersecurity practitioners to deliver a large end-to-end services
- Clients have raised concerns about CyberProof's limited domain training and talent skilling initiatives for its employees for cybersecurity capabilities

DXC Technology

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises looking for Microsoft-specific offerings may find DXC Technology relevant due to its Microsoft Defender services, underpinned by certified resources and robust partnership
- DXC Technology has invested in analytics in cybersecurity, allowing it to provide simplified security with contextualized persona-based actionable insights to the clients
- Enterprises from the autonomous vehicle industry seeking pure-play managed security services may find DXC Technology a suitable partner with its dedicated Virtual SoC (VSoC)-as-a-service offering
- Clients have appreciated DXC Technology's robust mix of offshore, onshore, and nearshore locations that allow it to pass on the cost benefits
- DXC Technology has invested in partnership-led co-innovative solution, Microsoft Copilot, in building gen AI capabilities in cybersecurity

Limitations

- DXC Technology lags its peers in investments in top-tier partnership with third-party technology providers such as Zscaler and checkpoint limiting its vendor-specific cybersecurity service offerings
- Enterprises looking for OT security offerings should carefully evaluate DXC Technology as it lacks maturity in capabilities such as remote access control, OT security assessments, and data security
- Enterprises seeking cybersecurity consulting services need to closely evaluate DXC Technology as it lacks pure-play consulting focus in cybersecurity
- Some clients have expressed concerns about DXC Technology's challenges with resource retention and the frequent changes in project staffing
- Clients have highlighted that DXC Technology lags its peers in network security services due to limited network security practitioners, platforms, and IP

EPAM

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises with cloud security services as key considerations may find EPAM to be a relevant provider because of its robust service offerings, underpinned by certified resources and accelerators such as SafeCloud Turnkey
- Enterprises seeking design and implementation capabilities in cybersecurity may find EPAM to be the right choice because of its specialized practitioners, backed by delivery proof points
- Enterprises from hi-tech and gaming industry seeking cybersecurity services may find EPAM relevant due to its credible delivery proof points and specialized resources
- Clients have lauded EPAM owing to its client management along with the strong domain knowledge in delivering cybersecurity services
- Few clients appreciated its innovative solutions such as identity life cycle governance, MLSecOps-as-a-service, and zero trust

Limitations

- Enterprises should be aware that EPAM lacks maturity in managed security services capabilities due to a limited SOC footprint, coupled with limited managed security resources
- Enterprises looking for cyber resiliency offerings should carefully assess EPAM as a suitable partner as it lags its peers in credible proof points in incident response and disaster recovery
- EPAM's limited platform-centric service offerings makes it a less suitable partner for enterprises looking for platform-led security services
- Some buyers have highlighted EPAM's premium pricing as a concern in cybersecurity services
- Enterprises from HLS, manufacturing, and the public sector should carefully evaluate EPAM as it has limited delivery proof point in these industries

Eviden

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises looking for vendor-specific IAM services can benefit from Eviden's well-structured technology-specific IAM offering such as Managed PKI Microsoft, IGAaaS SailPoint, and IGAaaS Evidian
- Eviden's Cyber Mesh platform-led MDR offering delivers managed security services, with enhanced flexibility, supported by automation
- Enterprises seeking industry-specific offerings may find Eviden pertinent because of its industry-specific cybersecurity offerings for verticals such as security for HLS and security for automotive
- Eviden IDaaS provides monitoring and reporting tools for enterprises to enhance compliance, bolster cyber resilience, and analyze network traffic
- Clients have appreciated Eviden owing to its technical expertise and competitive pricing

Limitations

- Enterprises seeking application security services should carefully assess Eviden as it lags its peers with limited automation
- Enterprises should be wary of Eviden's limited investments in building zero-trust security services
- Large enterprises seeking end-to-end cybersecurity services must be aware that Eviden has more focus on point solutions over holistic security
- A few clients have raised concerns around Eviden's ability to highlight areas of improvement beyond the immediate ask and does not come across as a strategic partner
- Clients have raised concerns around Eviden's premium pricing for cybersecurity services

Fujitsu

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises seeking strong managed security services offerings may find Fujitsu to be a suitable partner because of its several SOCs present in both offshore and onshore locations
- Fujitsu's focused investments in automation enable it to offer cost-optimized cybersecurity services to enterprises
- Enterprises may find Fujitsu to be a suitable partner for OT security as it offers end-to-end OT security services with its Protect the Parameter solution
- Enterprises searching for extensive cyber resilience services may benefit from its dedicated offering of continuity and resilience
- Fujitsu may be a relevant choice for enterprises seeking cloud security services as it has robust cloud security frameworks and platforms such as Springboard for secure cloud foundation

Limitations

- Enterprises seeking IAM services must carefully assess Fujitsu due to lack of demonstrable proof points in delivering services and limited enterprise mindshare
- Enterprises should carefully evaluate Fujitsu's cybersecurity consulting services as it lags peers in consulting-focused investments
- Fujitsu has limited focus on emerging cybersecurity themes, which curtails opportunities of enterprises requiring innovative service offerings such as zero trust, quantum computing, and DevSecOps
- Enterprises from niche industries should carefully evaluate Fujitsu, as it lacks industry-specific service offerings and has limited investment in emerging sectors such as autonomous vehicles and smart cities
- Enterprises with a high preference for regional delivery of cybersecurity services must carefully evaluate Fujitsu as it has limited onshore presence

GuidePoint Security

Everest Group assessment – Major Contender

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

- GuidePoint Security can be a preferred choice for enterprises seeking IAM services because of its dedicated consulting services offering, backed by certified practitioners
- Enterprises seeking application security may find GuidePoint Security to be relevant due to its automation-driven penetration testing capabilities, accredited by CREST for expertise in this area
- Enterprises can benefit from GuidePoint Security's platform-led cloud security assessment offerings such as SaaS security and cloud-readiness assessments
- Clients have appreciated GuidePoint Security's project management capabilities in long-term security services engagement
- Clients have lauded GuidePoint Security owing to its robust partnership ecosystem as it has region-focused partnerships such as with Tenable

Limitations

- Enterprises requiring specialized architecture-level cybersecurity must carefully evaluate GuidePoint Security as a relevant choice since it has limited zero-trust services
- Enterprises looking for pure-play managed security services must be aware about its lack of SOCs and scant delivery capabilities
- Enterprises must be wary of GuidePoint Security's limited investments in partnership-led co-innovation in cybersecurity
- Clients with a global presence have highlighted that it lags its peers in providing security services for other regions such as Europe and MEA due to its significant onshore presence
- Clients have highlighted the nascent maturity of GuidePoint Security's OT security capabilities compared to peers, with limited OT security solutions and frameworks

Happiest Minds

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises searching for end-to-end cloud security services may find Happiest Minds to be a relevant choice with its cloud-native network and application security, along with CSPM capabilities, backed by credible delivery proof points
- Happiest Minds has invested in OT security, enabling it to enhance its capabilities in high-demand areas such as risk assessments, IAM, and asset management
- Enterprises in early stages of gen AI adoption may find Happiest Minds to be pertinent, as it offers security solutions for gen AI offerings including an AI governance framework and AI model security testing services
- Happiest Minds is a suitable choice for enterprises adopting zero trust, with its consulting services to develop a tailored zero-trust implementation roadmap
- Happiest Minds' acquisition of Sri Mookambika Infosolutions has added competencies in security capabilities for the HLS sector enterprises

Limitations

- Enterprises must carefully assess Happiest Minds' managed security services offerings as it lags its peers in threat response capabilities with limited automation
- Enterprises from North America looking for localized delivery must be aware that Happiest Minds does not have a SOC in the region
- Enterprises from energy and utility sector should be wary of Happiest Minds' limited delivery proof points and enterprise mindshare in cybersecurity services
- Client have raised concerns about Happiest Minds' limited domain training and talent skilling initiatives for its resources for cybersecurity capabilities
- Clients have called out a scope of improvement in focus on simplified and cost-optimized security service offerings

Infosys

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises can benefit from Infosys' Cybersecurity Mesh Architecture (CSMA) framework in securing modern next-generation network assets
- Enterprises seeking services around next-generation themes such as quantum security and SASE services can benefit from Infosys' investments in these domains
- Infosys has invested in offensive cybersecurity initiatives such as the Infosys Innovation Network (IIN), which includes an enterprise-readiness module enhancing enterprise security
- Some clients have appreciated Infosys owing to its breadth of services, technical expertise, and competitive pricing
- Enterprises seeking IAM services may find Infosys to be a relevant choice due to its robust IAM advisory and governance offerings, supported by delivery proof points

Limitations

- Infosys has OT security capabilities such as OT/IoT SecOps and governance; however, it lags its peers in areas such as remote access control and asset management
- Enterprises from North America seeking localized delivery should note that Infosys has a limited SOC presence in the region and relies significantly on offshore delivery centers
- Enterprises seeking industrial SOCs should be wary that Infosys lags its peers in providing vertical-specific cybersecurity service offerings
- Enterprises searching for consulting and design implementation security services may find Infosys less relevant compared to its peers due to its limited enterprise mindshare
- While Infosys offers significant point solutions for MDR services, it lacks a single unified platform for these services

LTIMindtree

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises seeking cybersecurity consulting services may find LTIMindtree suitable with its emerging in-demand offerings such as cyber resilience consulting and gen AI consulting
- Enterprises looking for end-to-end, platform-led security services may find LTIMindtree to be a relevant service provider with its unified platform, LTIM Pinaacle, with multiple modules of cloud, data, OT security, and GRC
- LTIMindtree is a relevant partner for enterprises searching for digital identity assurance and governance with a zero-trust approach and automation playbooks
- LTIMindtree's large number of SOCs in North America enable it to provide extensive managed security services to enterprises
- Enterprises searching for a service provider with global delivery capabilities may appreciate LTIMIndtree's presence across onshore, offshore, and nearshore locations

Limitations

- Enterprises seeking OT security services must carefully assess LTIMindtree as it lags its peers in areas such as remote access control and asset management in OT security
- Enterprises seeking partnership-led cloud security services must carefully assess LTIMindtree as it lags its peers in partnerships with hyperscalers
- Some clients have highlighted that LTIMindtree has limited flexibility in commercial model in cybersecurity services engagements
- Some clients have highlighted that LTIMindtree lags its peers in investments in resource training and upskilling initiatives
- Some clients highlighted that LTIMindtree lags its peers in thought leadership and does not come across as a strategic partner

NTT DATA

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises may find NTT DATA to be a suitable choice for OT security services due to its robust partnership with OT native-security technology providers such as Armis, Claroty, and Nozomi Networks
- NTT DATA may be a relevant partner for the enterprises seeking IAM services with its robust IAM framework for hybrid cloud along with delivery proof points in CIAM
- Enterprises looking for managed security services may benefit from NTT DATA's unified MDR services, along with 50+ global SOCs across the globe
- NTT DATA is a suitable partner for enterprises looking for zero-trust offerings with its different zero-trust model based on the enterprise cybersecurity maturity
- Clients have appreciated NTT DATA's ability to bring a well-balanced delivery structure that has a robust mix of offshore, nearshore, and onshore delivery capabilities

Limitations

- Enterprises seeking cybersecurity consulting services should carefully evaluate NTT DATA due to its limited resources and delivery proof points
- Enterprises seeking gen AI security should be aware of NTT DATA's limited investments in building a gen AI security services portfolio
- A few clients have expressed concerns about NTT DATA's process-driven approach that prioritizes process over the response
- Some clients have highlighted that NTT DATA needs to play a more significant role in internal discussions and be a part of decision-making with senior stakeholders
- Enterprises from HLS vertical must carefully assess NTT DATA due to limited delivery proof points in this vertical compared to its peers

PwC

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises looking for DevSecOps services may find PwC relevant because of its robust consulting and implementation services around agile DevSecOps
- Enterprises may find PwC to be a suitable partner for cyber incursion preparedness with its cybersecurity simulation for network security and cloud security with Cyber Security Simulation Platform (CSSP)
- PwC is a pertinent choice for enterprises looking for risk management with its proprietary Cyber Risk Insights (CRI) platform
- Enterprises seeking threat intelligence capability may find PwC to be relevant with its threat intelligence platform backed by credible delivery proof points
- Clients from BFSI and manufacturing verticals have lauded PwC's technical expertise and domain knowledge

Limitations

- Enterprises with stringent budgets seeking cybersecurity services must be aware that PwC has premium pricing compared to peers
- PwC lags peers in investing in co-innovation infrastructure such as garages and technology hubs, which limits its capabilities to lead co-innovation with customers and proactively build Proofs of Concept (PoCs) cutting across multiple cybersecurity segments
- Clients have highlighted that PwC lags its peers in application security services and has limited enterprise mindshare
- Clients believe that it needs to invest more in embedding automation into its cybersecurity portfolio
- Enterprises seeking extensive flexibility and customization may encounter limitations in PwC's offerings, as they primarily rely on standardized solutions

Tech Mahindra

Everest Group assessment – Major Contender and Star Performer

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises seeking risk and compliance services may find Tech Mahindra to be a relevant partner due to its robust integrated GRC management framework
- Tech Mahindra has invested in emerging cybersecurity offerings such as quantum security services, SASE, and DevSecOps, building a strong security services portfolio
- Clients have lauded Tech Mahindra for its technical capabilities, domain understanding, and competitive pricing
- Clients have appreciated Tech Mahindra owing to its network security services and its telemetry coverage of network devices
- Enterprises may find Tech Mahindra to be pertinent with its consulting and design and implementation services

Limitations

- While Tech Mahindra has invested in data and network security, it lags in maturity regarding OT security capabilities and has limited delivery proof points
- Enterprises seeking cyber resilience should carefully assess Tech Mahindra, as it lags its peers in strategic roadmap for resilience implementation
- Enterprises searching for managed security services should carefully assess Tech Mahindra as it has limited SOCs compared to its peers
- Enterprises looking for a robust onshore-nearshore presence may find Tech Mahindra lagging its peers in providing a strong localized presence
- Tech Mahindra is a less suitable choice for enterprises seeking end-to-end cybersecurity services, as it lacks a unified platform for holistic security implementation and relies on multiple point solutions

Verizon

Everest Group assessment – Major Contender

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises seeking incident response may find Verizon to be a relevant service provider with its dedicated Verizon Threat Research Advisory Center (VTRAC) for incident response planning, honeypot reporting, and response offering
- Enterprises requiring pure-play cybersecurity services for mobile devices can benefit from Verizon’s dedicated mobile device management service, which offers telemetry coverage and data privacy for BYOD
- Enterprises with a high preference for localized delivery may find Verizon to be a suitable partner due to its strong onshore delivery footprint
- Enterprises may find Verizon to be pertinent because of its robust network security services with DDoS protection and telemetry coverage for IT and OT networks
- Enterprises in the BFSI sector may find Verizon to be a relevant choice due to its dedicated cloud security offering for mobile banking

Limitations

- Enterprises must be wary of Verizon as it lags its peers in IAM security services due to limited IAM practitioners and nascent frameworks
- Enterprises should carefully assess Verizon for governance and policy management services due to its limited investments in automation and lack of platform-led governance solutions
- Enterprises seeking platform-led security should carefully assess Verizon, as it relies on third-party security tools and lacks an in-house security platform
- Verizon’s limited investments in gen AI might result in significant gaps in services for enterprises in gen AI security
- A few clients have highlighted that Verizon lags its peers in highlighting areas of improvement beyond the immediate ask and does not come across as a strategic partner

WWT

Everest Group assessment – Major Contender

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

- Public sector enterprises may find WWT to be a pertinent choice due to its Unified Cyber Platform (UCP), making it suitable for the requirements of the modern federal defense clients
- WWT is a relevant choice for enterprises looking for OT security services as it has a strong partnership ecosystem with technology providers such as Armis, Forescout, and Claroty
- WWT's Managed Advisory Risk Services (MARS) provides executive-level cybersecurity oversight, making it a relevant choice for enterprises seeking risk management solutions
- Enterprises seeking cyber resilience services can consider WWT as it has defined service offerings with anticipate, withstand, recover, and adapt modules
- Enterprises with a high adoption of AI can benefit from WWT's security for AI offerings with compliance for data privacy and business continuity services

Limitations

- Enterprises seeking analytics-driven cybersecurity should carefully assess WWT as it has limited delivery proof points of proactive cybersecurity implementations
- Enterprises looking for industry-specific SOCs should carefully evaluate WWT, as it lacks industry-specific cybersecurity services offerings
- WWT lags peers in investments in training initiatives for upskilling and cross-skilling due to a limited partnership-led training programs with technology providers
- Clients have raised concerns about WWT's cloud security capabilities and resource skill gap
- A few clients have raised concerns around WWT's ability to highlight areas of improvement beyond the immediate ask and that it does not come across as a strategic partner

Enterprise sourcing considerations

Aspirants

- Aujas
- Harman
- Innova Solutions
- Orion Innovation
- Yash Technologies

Aujas

Everest Group assessment – Aspirant

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises seeking robust IAM services may consider Aujas as it has its flagship platform, Aujas PALM, backed by credible delivery proof points
- Aujas may be a relevant choice for the enterprises looking for application security and DevSecOps services owing to its AppSecure CoE, with specialized application security practitioners
- Enterprises can leverage Aujas' robust design and implementation security services offerings, underpinned by its specialist practitioners in secure architecture and system design
- Aujas has invested in building IP and accelerators such as Code Design and Shaksham, which allows it to offer simplified security to its clients
- Clients have lauded Aujas owing to its technical capabilities and domain knowledge, and competitive pricing

Limitations

- Enterprises should be wary of Aujas's limited capabilities in domains such as disaster recovery, network, and endpoint security
- Enterprises looking for pure-play managed security services may not find Aujas to be suitable as it has a relatively higher focus on consulting and design and implementation services
- A few clients have highlighted that Aujas has a lengthy contract renewal process
- Clients have raised concerns about Aujas's project management, noting issues of communication gap and misaligned resource allocation
- Enterprises from Canada and Mexico may not find Aujas relevant due to lack of proof points and enterprise mindshare in the region

Harman

Everest Group assessment – Aspirant

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises can benefit from Harman's endpoint security services, led by cybersecurity asset management platform Harman DefenSight and Harman SOC Copilot
- Enterprises seeking IoT/OT security may find Harman to be a relevant choice as it provides cybersecurity services with extensive delivery proof points in OT/IoT security assessments
- Enterprises seeking Microsoft-specific security services may find Harman a pertinent choice, due to its dedicated Cyber Defense Center compatible with the Microsoft tools stack
- Enterprises from the RCPG and hi-tech industries can benefit from its strong emphasis on avenues such as threat intelligence and incident response
- Clients have lauded Harman's technical and domain expertise, commercial flexibility, and overall account management

Limitations

- Enterprises with a demand for pure-play cybersecurity consulting services must carefully evaluate Harman as it has limited consulting specialized practitioners
- Enterprise from the public sector and HLS should be wary of Harman's limited cybersecurity services presence in the verticals
- Enterprises should be wary of Harman's limited partnerships with cybersecurity technology providers
- Enterprises searching for a service provider with localized talent should be aware that Harman's large pool of talent is mostly based out of offshore locations and has one SOC in North America
- Clients have highlighted that the Harman lags its peers in threat reporting capability

Innova Solutions

Everest Group assessment – Aspirant

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises may find Innova Solutions to be a partner of choice in OT security with its robust cybersecurity offerings embedded with zero trust and threat intelligence
- Enterprises can benefit from Innova Solutions' investments in gen AI for cybersecurity, allowing it to provide proficient offensive cybersecurity with user behavior using Neurosymoblic AI
- Enterprises from the BFSI and HLS industries may find Innova Solutions to be a suitable partner with its industry-specific offerings such as vulnerability management for HLS
- Clients have lauded Innova Solutions owing to its high talent retention
- Enterprises in early stages of gen AI adoption can benefit from Innova Solutions' dedicated consulting services for the safe adoption of gen AI

Limitations

- Enterprises must be aware that Innova Solutions has point solutions in managed threat detection and response such as SOAR workflow automation and threat response, and lacks unified threat detection and response capabilities
- Enterprises seeking design and implementation services must carefully assess Innova Solutions due to its limited capabilities and proof points
- Enterprises should be wary that Innova Solutions lags its peers in IAM security services with limited certified IAM practitioners and enterprise mindshare
- Clients have highlighted that Innova Solutions could enhance its services offerings with a focus on cost optimization
- Clients have highlighted that Innova Solutions lags its peers in cybersecurity expertise for niche industries such as mining

Orion Innovation

Everest Group assessment – Aspirant

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises in the telecommunications sector may find Orion Innovation to be a suitable cybersecurity service provider due to its proven expertise in network and IP security
- Enterprises seeking consulting services may find Orion Innovation to be pertinent due to its specialized practitioners and high-risk assessment proof points
- Orion Innovation's dedicated Cyber Defense practice, along with data security analytics for hybrid cloud, may be relevant for enterprises seeking cloud security services
- Some clients have highlighted that Orion Innovation has done significant investment in training and certifications of its resources
- Some clients have appreciated Orion Innovation's ability to provide quick and reliable cloud security posture management services

Limitations

- Enterprises seeking IAM services should carefully evaluate Orion Innovation, as it lags peers in mature frameworks-led solutions
- Enterprises searching for OT security must be aware that it lags peers in OT-specific partnerships with technology providers
- Enterprises must be aware that Orion Innovation has limited investments in emerging cybersecurity themes such as zero trust, quantum security, and SASE
- Orion Innovation may not be a preferred partner of choice for enterprises seeking platform-led security services due to its dependency on third-party tools
- Enterprises searching for managed security services should carefully evaluate Orion Innovation as it has limited SOC analysts and significant reliance on offshore delivery centers

Yash Technologies

Everest Group assessment – Aspirant

Measure of capability: ◔ Low ● High

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

Strengths

- Enterprises seeking application penetration testing services may find Yash Technologies to be a suitable partner, with its robust frameworks and credible delivery proof points
- Yash Technologies may be a relevant choice for enterprises seeking cybersecurity assessment services, underpinned by its Cyber Kill Chain Assessment Services
- Enterprises can benefit from Yash Technologies’ threat intelligence services, with its offensive cybersecurity approach and extensive delivery proof points
- Enterprises searching for managed security services may find Yash Technologies to be a relevant choice as it has robust service offerings such as dark web monitoring and malware sandboxing
- Enterprises seeking risk management can find Yash Technologies a strong partner for TPRM, risk monitoring, and governance services

Limitations

- Enterprises should carefully assess Yash Technologies’ OT security capabilities as it has limited telemetry coverage of OT and IoT assets
- Enterprises should evaluate Yash Technologies’ cloud security capabilities as it lacks enterprise mindshare due to limited credible delivery proof points compared to peers
- Enterprises must be aware that Yash Technologies’ lags its peers in terms of investments in innovative solutions in cybersecurity
- Enterprises seeking platform-led security should carefully assess Yash Technologies as it relies on third-party cybersecurity tools for implementation
- Enterprises should be wary of Yash Technologies’ limited delivery footprint around providing design and implementation services for a highly customized MDR technology stack

Appendix

Glossary

Research calendar

Glossary of key terms used in this report

DDoS	Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt traffic to targeted server, service, or network by overwhelming the target or the surrounding IT infrastructure with a flood of internet traffic
DevSecOps	Introducing security earlier in the software development life cycle to minimize vulnerabilities and bring security closer to IT and business objectives
EDR	Endpoint Detection and Response (EDR) detects and investigates suspicious activities on endpoints and employs a high degree of automation to quickly identify and respond to threats
Endpoint security	Includes protection of end-user devices (e.g., desktops, laptops, mobiles, and tablets), data protection, and Host Intrusion Prevention Systems (HIPS)
GRC	Governance, Risk Management, and Compliance
IAM	The Internet of Things describes the network of physical objects / things that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet
IoT	MDR stands for managed detection and response. It is an offering that combines four basic services – threat hunting, threat intelligence, incident detection and triaging, and incident response delivered from a cloud-based platform from Security Operations Center (SOCs)
MDR	MDR stands for Managed Detection And Response. It is an offering that combines four basic services – threat hunting, threat intelligence, incident detection and triaging, and incident response delivered from a cloud-based platform from SOCs
OT/ICS	Combination of computing and communication systems to manage, monitor, and control industrial operations. Focuses on physical devices and processes that they use
SOAR	A solution stack that allows an organization to collect security data from multiple sources and respond to security events without human assistance
Security Operation Center (SOC)	A centralized service provider unit for managing enterprise security issues by providing services such as security logs and event management, security incident response, malware analysis, and forensics
Threat intelligence platform	A platform that helps organizations aggregate, correlate, and analyze threat data from multiple sources in real time to support enterprise defensive actions

Research calendar

Cybersecurity

Published Current release Planned

Reports title	Release date
Cloud Security Services – Provider Compendium 2024	Jan 2024
gen AI Adoption in Cybersecurity	May 2024
Security – Review of Google Next ’24 Product Launch	May 2024
Operational Technology (OT) Security Products – Provider Compendium 2024	July 2024
Microsoft Security – Review of Microsoft Security’s Product Launch at RSAC ’24	July 2024
Cybersecurity Services PEAK Matrix® Assessment 2024 – North America	September 2024
Cisco – Review of Cisco Security’s Product Launch at RSAC ’24 and Cisco Live 2024	Q3 2024
Cybersecurity Services Specialists PEAK Matrix® Assessment 2024	Q3 2024
Cybersecurity Services PEAK Matrix® Assessment 2024 – Europe	Q4 2024
Cybersecurity Services Specialists Compendium 2024	Q4 2024
Cybersecurity Services Provider Compendium 2024 – North America	Q4 2024
Cybersecurity Services Provider Compendium 2024 – Europe	Q4 2024
Managed Detection and Response (MDR) Services PEAK Matrix® Assessment 2024	Q4 2024
Managed Detection and Response (MDR) Services Compendium 2025	Q1 2025

Note: Click to see a list of all of our published Cybersecurity reports

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.

Everest Group®
With you on the journey