



HORIZONS REPORT

# Cybersecurity Services, 2025

**An assessment of the leading service providers in cybersecurity resilience and innovation**

**Authors:**

Akshat Tyagi, Associate Practice Leader  
Jason Dann, Research Analyst  
Ashwin Venkatesan, Executive Research Leader  
Mayank Madhur, Practice Leader

Excerpt for EY

“

Cybersecurity expectations have evolved. It is no longer enough for service providers to just protect infrastructure. They are now evaluated by how effectively they reduce risk, accelerate response, and enable measurable business impact. This demands a shift from monolithic managed services to modular, outcome-driven solutions that combine automation, domain context, and decision intelligence.

What sets top-performing providers apart is their ability to translate that shift into practice. They build integrated cyber strategies that align with enterprise risk priorities, deliver situational awareness, and help clients make informed decisions under pressure. The goal is resilience: keeping the business running even when under attack.

”



**Akshat Tyagi**

Associate Practice Leader,  
HFS Research

“

The cybersecurity market is consolidating fast, not just in tooling but in trust. Buyers are demanding fewer providers, broader accountability, and outcomes they can measure. Our research makes it clear: the next winners in cyber are not those with the most logos but those who deliver platformized, budget-rationalized services that scale across identity, cloud, and threat response.

”



**Ashwin Venkatesan**

Executive Research Leader,  
HFS Research

# Table of contents

	Page
<b><u>SECTION 01</u></b>	
Introduction and research methodology	04
<b><u>SECTION 02</u></b>	
Market dynamics	14
<b><u>SECTION 03</u></b>	
Horizons results: Cybersecurity services, 2025	22
<b><u>SECTION 04</u></b>	
EY profile: Cybersecurity services, 2025	25
<b><u>SECTION 05</u></b>	
HFS Research authors	27

# 1

## Introduction and research methodology

# Introduction

- Organizations of all sizes are increasingly prioritizing proactive cybersecurity strategies. This means a growing focus on real-time threat detection, enhanced data protection, and developing resilient digital environments. To achieve these outcomes, enterprises often turn to service firms to help them plan, implement, and manage cybersecurity solutions.
- The **HFS Horizons: Cybersecurity Services, 2025** report assesses how well service providers are helping their cybersecurity clients to embrace innovation and realize value across three distinct Horizons:
  - **Horizon 1**– Ability to support security enhancement of **digital estates** while helping **reduce the costs of cybersecurity delivery** with relevant offerings.
  - **Horizon 2** - Horizon 1 + the ability to drive the '**OneOffice**' mindset to **break down the barriers** imposed by the value chain and develop **a contextual and adaptable security posture**.
  - **Horizon 3** - Horizon 2 + the ability to drive the '**OneEcosystem**' approach to enable a **comprehensive, predictive** security posture considering **dynamic business needs and evolving threat landscapes**.
- The report evaluates the capabilities of **24 service providers** across the HFS Cybersecurity services value chain based on a range of dimensions to understand the **why, what, how, and so what** of their offerings.
- It highlights the **value-based positioning** for each participant across the three distinct Horizons. It also includes **detailed profiles** of each service provider, outlining their **provider facts, strengths, and development opportunities**.
- The report is **global in scope** and offers critical insights for enterprises of all shapes and sizes, service providers offering cybersecurity services, and ecosystem partners navigating the rapidly evolving threat landscape.

# Executive summary (1/2)

The cybersecurity services market is evolving from reactive threat defense to proactive, business-aligned resilience. Enterprises now operate across hybrid IT estates, AI-enabled workflows, and increasingly regulated landscapes that raise the stakes for continuous protection and risk visibility. Buyers prioritize outcomes such as continuous threat exposure management (CTEM), secure digital transformation, and AI risk governance. Leading providers are responding with platformized delivery, industry-specific offerings, and strategic ecosystem alliances to address talent gaps and reduce complexity across fragmented environments.

- 1 The leaders**

HFS assessed 24 cybersecurity service providers across value propositions, innovation capabilities, go-to-market strategies, and market impact criteria. The nine Horizon 3 leaders are Accenture, Deloitte, Atos, EY, HCLTech, IBM, Infosys, TCS, and Wipro. These providers consistently enable enterprise-wide cybersecurity transformation through platform-driven services, zero trust integration, AI-augmented operations, and embedded compliance. Common characteristics among the leaders include deep domain expertise, strong global delivery models, co-innovation with clients, and robust ecosystem partnerships that enable resilience and security at scale.
- 2 Risk-to-resilience approach**

Enterprises are shifting their cybersecurity priorities from isolated threat prevention toward broader business resilience. Leading providers are responding with risk-informed strategies that embed cybersecurity into enterprise transformation journeys. They offer cyber fusion models, attack surface visibility, exposure quantification, and real-time remediation roadmaps aligned with business KPIs. This approach allows organizations to shift from reactive controls to proactive, trust-enabling programs that directly support operational continuity and regulatory mandates.
- 3 CTEM and exposure management gain ground**

Continuous threat exposure management (CTEM) is emerging as a central framework in modern cybersecurity delivery. Providers are offering structured CTEM programs that include asset discovery, validation of exploitability, contextual risk scoring, and automated remediation tracking. This model allows enterprises to replace traditional checklist-driven audits with ongoing, intelligence-led assessments prioritizing what matters most. As buyers look to move beyond alert fatigue and compliance box-ticking, CTEM is gaining traction as a path to measurable cyber maturity.
- 4 Security for AI becomes top of mind**

As enterprises adopt GenAI and other machine learning models at scale, the need to secure these assets is skyrocketing. Providers are launching dedicated services for securing AI models, data pipelines, and outputs. Offerings include red teaming of large language models, bias detection, AI governance frameworks, and compliance reporting for evolving regulations. Buyers increasingly prioritize explainability, auditability, and control over AI systems, pushing cybersecurity to intersect with data governance and ethics programs.

# Executive summary (2/2)

- |   |  |   |
|---|--|---|
| 5 | <b>Platformization and IP-led delivery</b>                     | Cybersecurity services are increasingly being delivered through integrated platforms rather than siloed engagements. Leading providers are building proprietary tools, accelerators, and orchestration frameworks that support automation across threat detection, vulnerability management, and identity governance. This platformization helps reduce time to value, improves consistency, and enables scalable delivery across geographies. It also supports outcome-based pricing and service models, which are in growing demand from enterprise buyers seeking predictability and efficiency. |
| 6 | <b>Vertical context and OT or IoT specialization</b>           | Industry-specific cybersecurity capabilities are becoming a competitive necessity, particularly in manufacturing, energy, healthcare, and BFSI sectors. Providers are investing in operational technology (OT) security playbooks, regulatory alignment frameworks, and domain-specific controls tailored to vertical threat environments. From protecting industrial control systems to ensuring patient data security and financial fraud resilience, buyers now expect providers to bring deep contextual understanding of their operating landscape and technical expertise.                    |
| 7 | <b>Talent strategy as a competitive lever</b>                  | With cybersecurity talent in short supply globally, providers are focusing on building resilient talent strategies as a core differentiator. This includes the development of cyber academies, partnerships with academic institutions, and internal reskilling initiatives to retain and redeploy skilled analysts. Many are also investing in nearshore and onshore SOC's to meet regulatory and client proximity needs. Buyers increasingly assess provider talent not just in terms of numbers but on specialization, continuity, and the ability to scale high-complexity engagements.         |
| 8 | <b>Emerging technologies reshape cybersecurity foundations</b> | Innovation is accelerating across the cybersecurity stack as providers invest in emerging technologies to prepare for future threats. Post-quantum cryptography, adaptive defense orchestration, self-healing environments, and automation into agentic workflows are beginning to enter enterprise roadmaps. Providers are also embedding AI governance and data privacy automation into core offerings. As threat actors evolve and regulation tightens, providers that invest in future-facing architectures will be best positioned to support enterprise security transformation.              |
| 9 | <b>Voice of clients and partners</b>                           | Clients and partners continue to value providers for their execution strength, operational discipline, and ability to reduce risk. However, they also seek more transparent roadmaps, co-creation opportunities, and better alignment of security strategy with business outcomes. Buyers want clearer articulation of service packaging, faster time to engagement, and active collaboration on emerging risk areas such as AI and OT. Providers combining dependable delivery with thought leadership and flexibility are more likely to earn long-term trust.                                    |



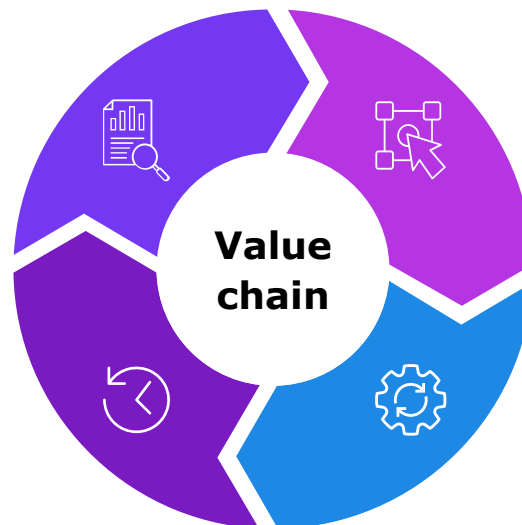
# The HFS cybersecurity value chain visualizes all steps from concept to management to performance measurement

## Assessment and readiness

- Cybersecurity strategy and transformation
- Security posture assessment and audits
- Board and business readiness (risk, regulations, compliance)
- Governance, risk, and compliance framework
- Framework, policies, and processes
- Target operating model
- Target technical architecture
- Technical feasibility and prototyping
- Cybersecurity personnel readiness and training
- Mergers, acquisitions, and disentanglements
- Disaster recovery

## Continuous improvement and innovation

- Emerging security technology evaluations and pilots (including securing AI / GenAI)
- Development of security playbook automation and orchestration
- Security integration and engineering
- Strategic partnerships and alliances
- Proprietary technology and IP development
- Security operation center transformation
- Information-sharing ecosystem and threat exchange
- Learning and training program
- Cybersecurity co-innovation labs and hubs
- Startups and academic collaboration



## Design and deployment

- Cyber risk management
- Infrastructure and end-point security
- Application security
- Digital identity and access
- Decentralized security
- Information security compliance
- Data privacy and protection
- Cloud risk and security
- Operational tech security
- Vulnerability detection
- Threat intelligence and analytics
- Threat hunting and offensive security
- Threat response and recovery
- Investigation and forensics
- Next-gen security (SASE, Gen AI security, confidential computing, quantum security)

## Maintenance and support

- Infrastructure, endpoint and network security support, and managed services
- Application and data security support and managed services
- Cloud security support, governance, and managed services
- Digital identity and access support and managed services
- IoT and OT security support and managed services
- Risk and compliance support and managed services
- Detection and response support and managed services
- Threat intelligence and hunting support, and managed services
- Digital forensics support and managed services
- Cybersecurity training support and managed services



# The HFS cybersecurity value chain defined

HFS developed the industry value chain concept to graphically depict our understanding of the processes and functions required to deliver key outcomes and operate the business.

The value chain for cybersecurity provides a comprehensive overview of services delivered through sophisticated cybersecurity across business functions in response to today's dynamic and evolving threat landscape.

## Assessment and readiness



Services to assist customers in assessing their cybersecurity posture and preparing to embark on large-scale cybersecurity initiatives. This phase prepares enterprises to face risks by identifying vulnerabilities, aligning strategies with regulatory requirements, and prioritizing action to ensure a solid foundation for resilience.

## Design and deployment



Services to assist customers in designing and deploying cybersecurity initiatives. This focuses on creating tailored security frameworks, integrating advanced technologies, and ensuring implementation to effectively combat current and emerging threats.

## Maintenance and support



Services to assist customers in managing day-to-day operations and keep their cybersecurity environment updated with the changing threat landscape. Each level includes proactive monitoring and continuous system optimization to provide regular updates and ensure sustained protection.

## Continuous improvement and innovation



Services to assist customers in improving their cybersecurity posture and embedding innovative practices and technologies into their existing environment. Build on the foundation of successful protection by leveraging advanced analytics, integrating emerging technologies, and fostering a culture of ongoing innovation to stay ahead of evolving threats and regulatory demands.

## 24 service providers have been evaluated in this report

**accenture**

**a** amdocs

**Atos**

birla**soft**

Capgemini

**cognizant**

Cyber**Proof**<sup>®</sup>  
A UST Company

**Deloitte.**

**DXC**  
TECHNOLOGY

**EY**  
Shape the future  
with confidence

**FUJITSU**

**HCLTech**

**HEXAWARE**

**Hitachi Digital Services**

**IBM**

**Infosys**<sup>®</sup>

**LTIMindtree**

**Mphasis**  
The Next Applied

**NTT DATA**

**orange** **Cyberdefense**

**tcs** **TATA**  
CONSULTANCY  
SERVICES

**TECH**  
**mahindra**

**unisys**

**wipro**

Note: All service providers are listed alphabetically

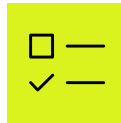
# Sources of data

This Horizons research report relies on multiple data sources to support our methodology and help HFS obtain a well-rounded perspective on the service capabilities of the participating organizations covered in our study. The sources are as follows:



## Briefings and information gathering

HFS conducted detailed **briefings** with cybersecurity leadership from each vendor. Each participant submitted a specific set of **supporting information** aligned to the assessment methodology.



## Reference checks

We conducted reference checks with **25 active clients and 32 active partners** of the study participants via surveys and interviews.



## HFS Pulse

Each year, HFS fields multiple demand-side surveys in which we include detailed vendor rating questions. For this study, we leveraged our fresh-from-the-field HFS Pulse study data featuring **305 enterprise leaders**.



## Other data sources

**Public information** such as news releases and websites. **Ongoing interactions, briefings, virtual events**, etc., with in-scope vendors and their clients and partners.

# The study seeks to address multiple questions

## Contextualized security

How are you orchestrating your offerings to support the dynamic business needs and contextual security requirements of individual clients? How are you helping clients conform to the ever-evolving global, local, and industry-specific data privacy laws and regulations?

## AI and GenAI security

How are you helping clients adapt to a rapidly evolving threat landscape driven by AI and GenAI adoption such as data leakage, application vulnerability, content anomalies, copyright issues, transparency and trust, and secure ModelOps?

## Hybrid IT infrastructure security

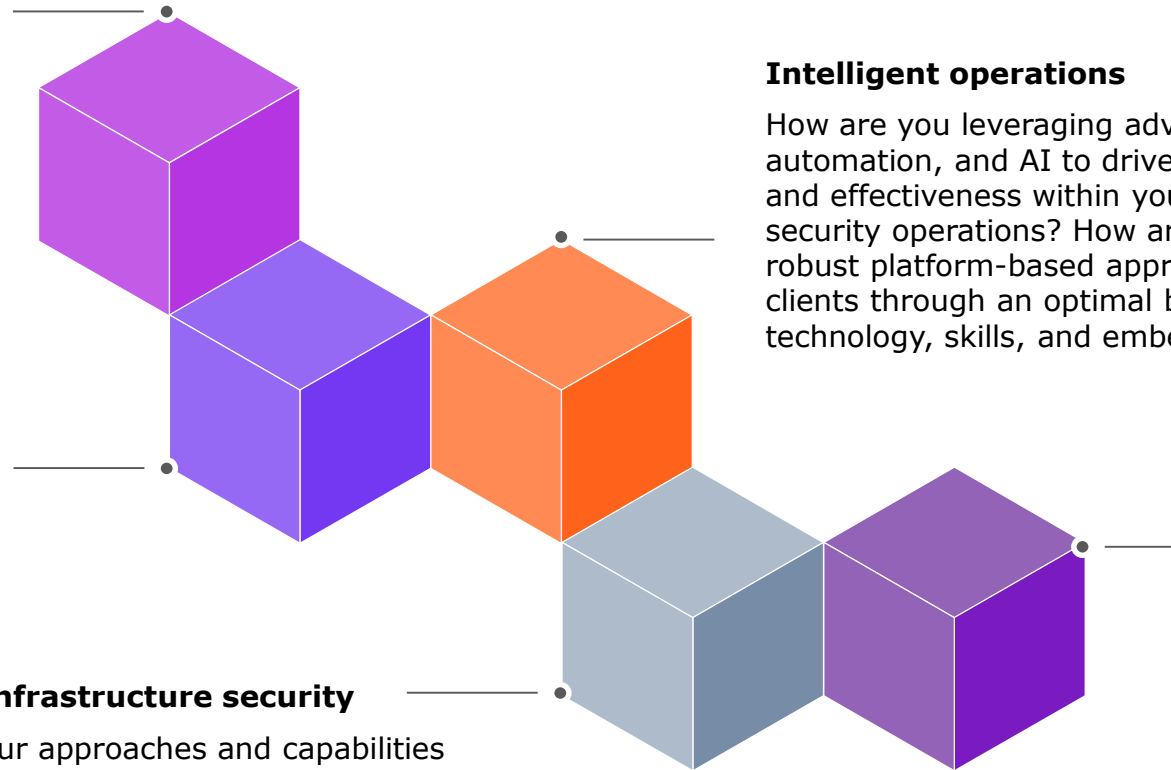
What are your approaches and capabilities for supporting clients in securing their complex IT infrastructure estates across traditional devices, cloud, SDx, edge and IoT networks, decentralized workloads, and other next-gen infrastructure components?

## Intelligent operations

How are you leveraging advanced analytics, automation, and AI to drive contextualization and effectiveness within your managed security operations? How are you enabling a robust platform-based approach for your clients through an optimal balance of technology, skills, and embedded context?

## Cybersecurity funding

How are you helping clients maximize value from limited security funds? What investments are you making to position yourself as a true cybersecurity partner (vs. services provider) to garner greater client spend?



# Horizons assessment methodology—cybersecurity service providers

The HFS Horizons: Cybersecurity Services, 2025 report evaluates providers' capabilities across a range of dimensions to understand the **why, what, how, and so what** of service offerings.

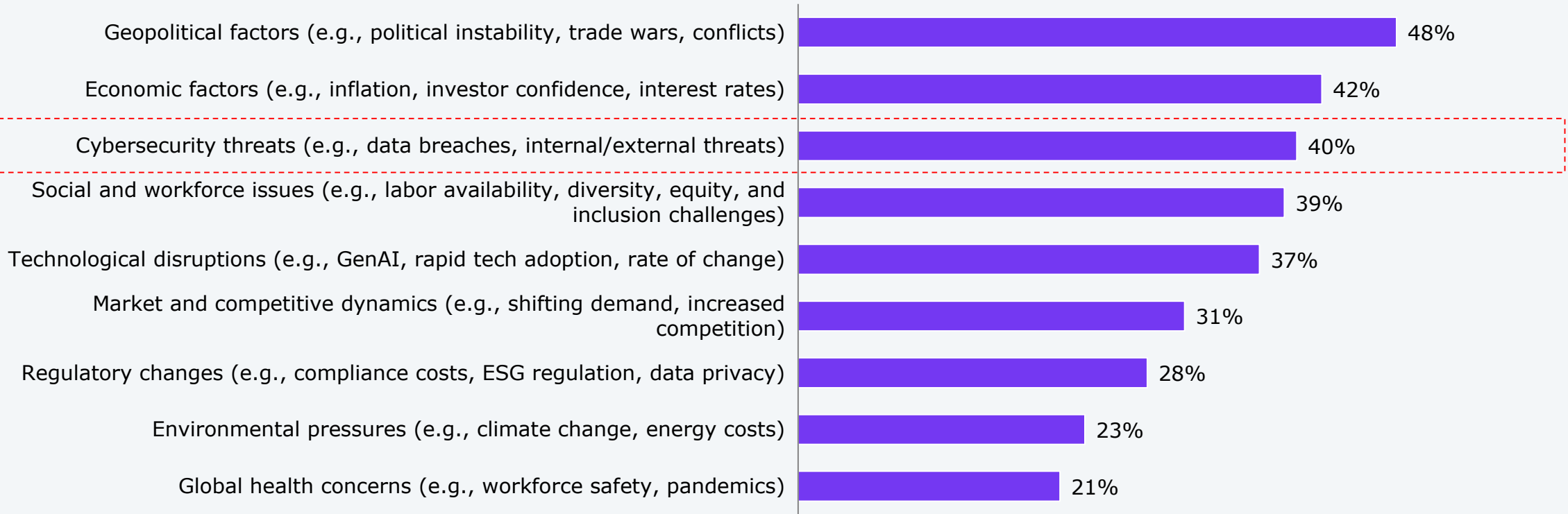
Assessment dimension (weighting)				
Distinguishing service provider characteristics	Value proposition: The why? (25%)	Execution and innovation capabilities: The what? (25%)	Go-to-market strategy: The how? (25%)	Market impact: The so what? (25%)
	<ul style="list-style-type: none"> <li>Strategy and roadmap</li> <li>Clarity of vision for cybersecurity and nature of outcomes</li> <li>Differentiators—why clients work with you</li> </ul>	<ul style="list-style-type: none"> <li>Breadth and depth of services across the cybersecurity value chain</li> <li>Integration of transformation and process consulting</li> <li>Approach to and strength of the ecosystem of partners</li> </ul>	<ul style="list-style-type: none"> <li>What transformation outcomes are you pitching to clients?</li> <li>Nature of investments in cybersecurity (M&amp;A, training, R&amp;D)</li> <li>Co-innovation and collaboration approaches with customers and partners including creative commercial models</li> </ul>	<ul style="list-style-type: none"> <li>Scale and growth of cybersecurity business; revenue, clients, and headcount</li> <li>Proven outcomes showcasing transformation enabled through cybersecurity</li> <li>Voice of the customer</li> </ul>
	Horizon 3	Horizon 2 +	Horizon 2 +	Horizon 2 +
	<ul style="list-style-type: none"> <li>Horizon 2 +</li> <li>The ability to drive the 'OneEcosystem' approach to enable a comprehensive, predictive security posture considering dynamic business needs and evolving threat landscapes.</li> </ul>	<ul style="list-style-type: none"> <li>Horizon 2 +</li> <li>Strategy through execution at scale</li> <li>Enabling continuous innovation to help enterprises stay at the forefront of technology and transformation</li> <li>Well-rounded capabilities across all value creation levers: talent, domain, technology, data, and change</li> </ul>	<ul style="list-style-type: none"> <li>Horizon 2 +</li> <li>Driving co-creation with clients and ecosystem partners</li> <li>Effectively envisioning outcomes and providing business assurance for transformation</li> </ul>	<ul style="list-style-type: none"> <li>Horizon 2 +</li> <li>Referenceable and satisfied clients driving new business models with the partnership</li> </ul>
Horizon 2	<ul style="list-style-type: none"> <li>Horizon 1 +</li> <li>The ability to drive the 'OneOffice' mindset to break down the barriers imposed by the value chain and develop a contextual, adaptable security posture.</li> </ul>	<ul style="list-style-type: none"> <li>Horizon 1+</li> <li>The ability to support clients on their transformational journey</li> <li>Global capabilities with strong consulting skills and partnerships with major hyper-scalers</li> <li>Range of industry-specific partnerships and strong PX</li> <li>Strong industry-specific IP</li> </ul>	<ul style="list-style-type: none"> <li>Horizon 1+</li> <li>Proven and leading-edge proprietary assets, including different platforms</li> <li>Clear articulation of the operating model</li> <li>Capability to deliver transformation</li> </ul>	<ul style="list-style-type: none"> <li>Horizon 1+</li> <li>Referenceable and satisfied clients for the ability to blend technology and business objectives</li> </ul>
	Horizon 1	Horizon 1	Horizon 1	Horizon 1
	<ul style="list-style-type: none"> <li>The ability to support the security enhancement of digital estates while helping to reduce the costs of cybersecurity delivery with a relevant set of offerings.</li> </ul>	<ul style="list-style-type: none"> <li>Strong implementation capabilities and managed services partners.</li> <li>Deep engineering capabilities driving speed and efficiency</li> <li>Offshore-focused with strong technical skills</li> <li>Focused partnerships and strong PX</li> <li>Some industry-specific IP</li> </ul>	<ul style="list-style-type: none"> <li>Robust fundamentals of technology transformation</li> <li>Technology and capability focus</li> </ul>	<ul style="list-style-type: none"> <li>Referenceable and satisfied clients for the ability to execute technology transformation</li> </ul>

# 2

## Market dynamics

# Cybersecurity threats rank among leading barriers to enterprise progress

What are the most concerning external factors impacting your organization’s ability to achieve its priorities?



Sample: 305 major enterprise decision makers  
Source: HFS Research Pulse, 2025



# Top challenges for cybersecurity enterprise clients in 2025

## Complexity and expansion of attack surfaces

1

Enterprises face challenges in continuously mapping and monitoring a sprawling, dynamic attack surface that includes cloud, IoT, and hybrid environments, increasing exposure to sophisticated and targeted threats.

## Managing identity as the new perimeter

2

With the rise of cloud, remote work, and third-party access, identity has become the frontline of enterprise security. However, gaps in control and visibility still make it hard to manage who gets access to what while keeping it that way.

## Quantifying cybersecurity ROI under budget pressures

3

Organizations must optimize cybersecurity investments under tighter budgets and staffing constraints. Boards now demand measurable outcomes and defensible ROI, not activity metrics, making it harder for CISOs to justify spend without a clear impact.

## Regulatory compliance and governance

4

Rapidly evolving regulations across multiple jurisdictions require enterprises to continuously update compliance frameworks, automate reporting, and manage risks to avoid penalties and reputational damage.

## Speed and efficiency of threat detection and response

5

Enterprises struggle with slow detection and remediation cycles, often taking months to resolve critical vulnerabilities, which increases the window of exposure to cyberattacks.

## Emerging risks in GenAI/agent AI security

6

Enterprises are rapidly adopting GenAI without securing it. Data leakage, model manipulation, and lack of AI governance create new, poorly understood attack surfaces. Model-level security (e.g., prompt abuse, jailbreak detection) is still rare.

# Evolving enterprise expectations and pain points

Trend	Demand side (enterprise expectations)	Supply side (provider offerings)	Key pain points to address
<b>AI and automation in security</b>	Enterprises expect advanced AI and GenAI for proactive threat detection, alert summarization, response automation, and securing AI systems (e.g., LLMs, hallucinations, prompts).	Providers are integrating AI/ML into MDR, SOAR, and orchestration. Some have begun GenAI-based SOC tooling and AI red teaming.	<ul style="list-style-type: none"> <li>• Clients need GenAI that’s explainable and production-ready</li> <li>• Trust must improve through stronger validation and safeguards</li> <li>• Clearer regulatory guidance for secure AI use</li> </ul>
<b>Zero trust and identity security</b>	Enterprises want full-stack zero trust across identity, data, apps, and OT, including passwordless IAM, risk-based policies, and unified role orchestration.	Vendors offer strong zero trust maturity models, identity orchestration (e.g., sub-60 sec provisioning), and compliance-backed advisory services.	<ul style="list-style-type: none"> <li>• Enterprises need help modernizing identity and legacy systems</li> <li>• Unified IAM enforcement across IT, cloud, and OT is essential</li> <li>• Policy orchestration must improve across fragmented setups</li> </ul>
<b>Cloud-native and multi-cloud security</b>	Clients demand consistent visibility, posture control, and data security across hybrid, public cloud, and edge environments, including container and serverless workloads.	Providers supply cloud-native security platforms, SASE, CNAPP, and hybrid cloud security solutions. CSPM is also maturing.	<ul style="list-style-type: none"> <li>• Clients seek unified visibility across complex hybrid-cloud setups</li> <li>• CSP-specific tools lack unified security oversight</li> <li>• Posture control must align with audit and trust requirements</li> </ul>
<b>Regulatory compliance and risk management</b>	Enterprises expect embedded compliance for DORA, NIST2, SEC rules, PCI-DSS, and region-specific regulations with audit-ready evidence and automated GRC flows.	Providers offer compliance consulting and control mapping, with early efforts toward automation and sector-specific risk scoring.	<ul style="list-style-type: none"> <li>• Coverage struggles to keep up with fast-evolving mandates</li> <li>• Need localized support for jurisdiction-specific mandates</li> <li>• GRC tools must automate evidence generation and mapping</li> </ul>
<b>Managed security services (MSS) and cyber resiliency</b>	Buyers now demand modular, SLA-driven MSS with embedded advisory, GenAI-powered orchestration, self-healing playbooks, and cyber recovery-as-a-service.	Most vendors provide SOCs, MDR/XDR, and bundled MSS offerings, with limited use of GenAI or shared outcome models.	<ul style="list-style-type: none"> <li>• Buyers want MSS offerings with agility and tailored response</li> <li>• Expect SLA-backed GenAI-driven security</li> <li>• Need stronger focus on risk ownership and recovery outcomes</li> </ul>

# What enterprises really want from cybersecurity providers?

## **Business-aligned risk reduction over technical coverage**

Enterprises want providers to show which business systems or applications are at risk, not just share patch status, CVSS scores, or threat counts.

## **Modular, composable services over rigid MSSP contracts**

Clients increasingly prefer cybersecurity services flexibly tailored to evolving needs, with SLAs for specific use cases instead of bundled 'black-box' offerings.

## **Securing the AI stack, not just using it for detection**

It's no longer enough to use GenAI for analytics; buyers want assurance that their own AI tools are governed, protected from prompt injection, and tested for model-level vulnerabilities.

## **Outcome metrics over activity dashboards**

CISOs are under pressure to justify cyber spend to the board and expect providers to quantify actual risk reduction, not just operational activity or alert volumes.

## **Orchestrated response ownership over alerts-only SOC**

Enterprises want more than 24/7 monitoring, i.e., they expect providers to own time-bound containment, recovery steps, and root-cause accountability within the SOC workflow.

# Key trends across the study (1/2)

1

## **AI and automation-driven security operations**

AI/ML and GenAI are transforming cybersecurity by enabling faster threat detection, automated incident response, and intelligent compliance orchestration. Enterprises now expect platforms to reduce operational effort, accelerate mean time to resolution (MTTR), and integrate with human-led workflows. Emerging needs include securing GenAI systems, such as hallucination control and prompt injection defense. Instead of asking for more detection tools, buyers want a measurable reduction in MTTR, for e.g., 25%, with fewer false positives.

2

## **Zero trust security architectures**

Zero trust models are widely embraced to reduce lateral movement and secure hybrid, multi-cloud, and OT environments. Buyers prioritize continuous authentication, privilege enforcement, and centralized identity orchestration. However, organizations face execution challenges across legacy infrastructure and fragmented control systems.

3

## **Cloud-native and hybrid multi-cloud security**

As cloud adoption accelerates, enterprises demand consistent visibility and unified policy management across cloud workloads, containers, and OT/IT. Providers offer SASE, CNAPP, and DSPM, but managing posture across CSPs remains complex, often causing gaps in visibility and response.

4

## **Regulatory compliance and industry-specific security**

Evolving regulations (e.g., DORA, NIST2, SEC rules) push demand for embedded compliance. Enterprises now expect plug-and-play blueprints with pre-audited controls and industry-specific frameworks. Automation in risk quantification and GRC is essential for audit readiness.

## Key trends across the study (2/2)

5

### **Managed detection and response (MDR) and co-managed security services**

Clients are moving beyond basic MDR to seek SLA-driven, modular security services that include GenAI-powered playbooks, recovery automation, and embedded advisory. Traditional 24/7 SOC models are being replaced by flexible, outcome-aligned MSSP delivery.

6

### **Integration of emerging technologies from AI-enhanced to quantum-safe security**

Security providers invest in quantum-resistant cryptography and AI-driven threat detection to stay ahead of evolving attack vectors. In parallel, enterprises now demand controls to secure AI, including LLM red teaming, hallucination prevention, and GenAI model governance.

7

### **Focus on identity and access management (IAM) and privileged access**

IAM remains a cornerstone of enterprise security strategies. Clients expect fast, policy-driven onboarding, CIAM/PAM integration, and IAM orchestration to enforce zero trust across users, devices, and applications, especially in hybrid and regulated environments.

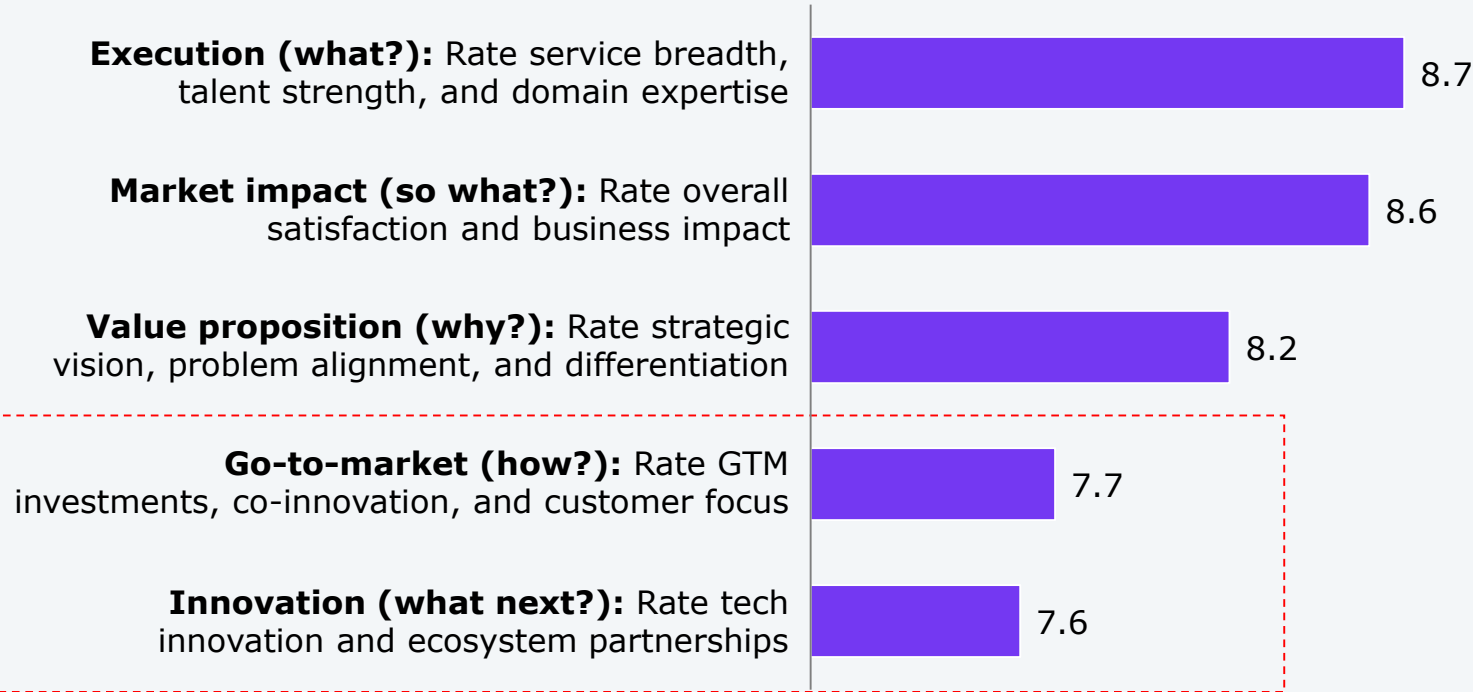
8

### **Cybersecurity for OT/IoT and industrial environments**

With the growing convergence of IT and OT systems, enterprises seek specialized security for ICS, connected devices, and critical infrastructure. Challenges include asset visibility, segmenting legacy protocols, and extending IT controls (e.g., SOAR, ZTNA) into air-gapped or proprietary OT environments. Deepfake-driven impersonation and AI-generated content pose a growing risk to ICS and OT sectors reliant on manual identity verification and human supervision.

# Client ratings reveal weak spots in innovation and market approach

**Clients: Rate the following aspects of the service provider on a scale of 1 to 10 (1 being the lowest and 10 as the highest; weighted average of ratings)**



Clients suggest that while providers perform well operationally, they may not be doing enough to communicate their vision, investment focus, or the full scope of their capabilities. It may also reflect a gap in how providers involve clients in shaping forward-looking solutions. This is a gentle signal to improve how strategy and innovation are brought into client conversations.

Sample: 25 active client references of the study participants  
Source: HFS Research, 2025

# 3

## Horizons results: Cybersecurity services, 2025



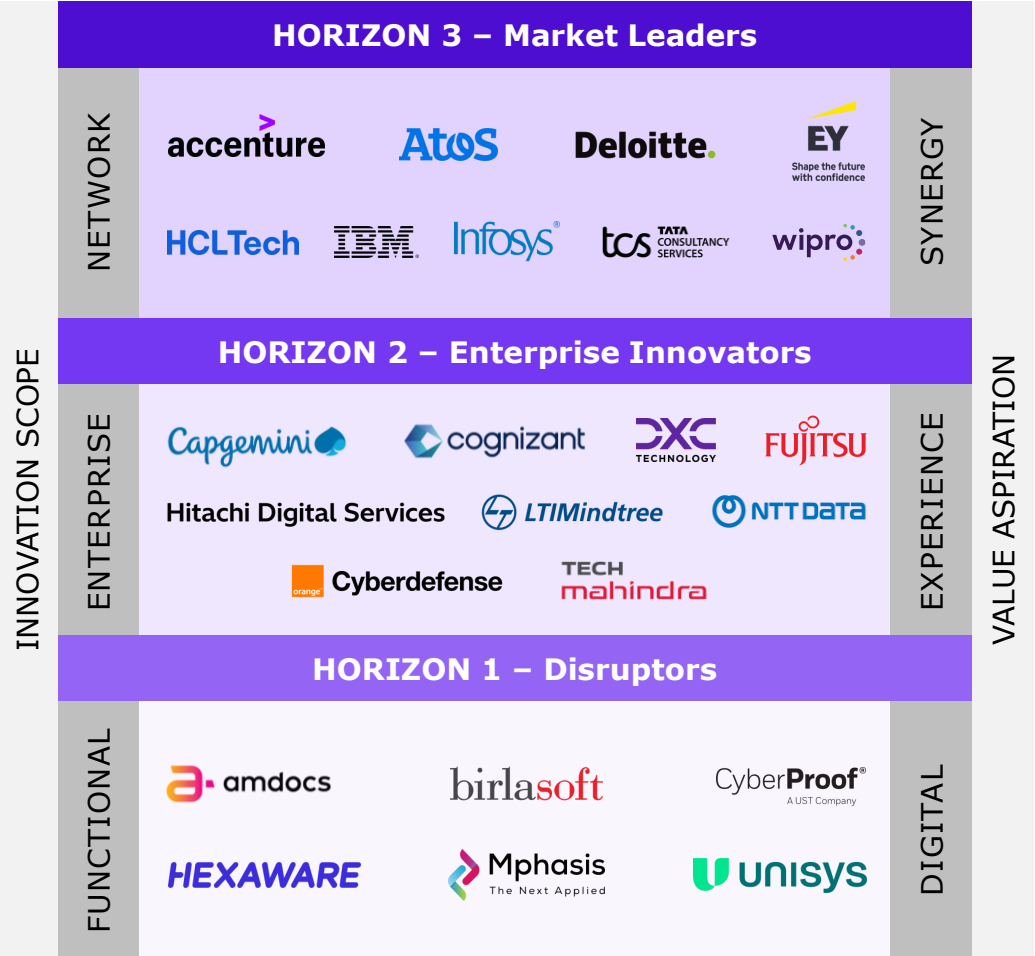
# HFS Horizons: Summary of providers assessed in this report

Providers	HFS point of view
Accenture	Leverages Cyber Fusion Centers and AI-driven simulations to deliver transformation at scale through platform-led security
Amdocs	Delivers telco-focused cybersecurity with 5G security, zero trust integration, and partner-led resilience
Atos	Delivering sovereign cybersecurity with post-quantum encryption, identity innovation, and audit-proven resilience at scale
Birlasoft	Focuses on compliance-led industrial cybersecurity with SAP, IAM, and emerging IT-OT risk convergence at scale
Capgemini	Enabling secure digital modernization with AI-powered services, global CDCs, and scalable compliance accelerators
Cognizant	Delivers scalable MSS and OT-to-cloud protection through industrialized platforms and compliance-first execution
CyberProof	Delivers threat exposure-led cybersecurity with AI-driven analysis, automation, and co-managed defense operations
Deloitte	Empowering enterprises to transform securely and confidently with integrated, future-ready cybersecurity for IT, cloud, and OT environments
DXC	Embedding security across IT, cloud, and OT with AI-driven architecture and zero trust resilience
EY	Drives board-level cyber alignment through GRC, AI assurance, and consulting-first delivery models
Fujitsu	Delivers cybersecurity with CTEM, sovereign cloud, IT-OT controls, and automation-backed visibility
HCLTech	Empowering enterprise transformation with GenAI, zero trust, CTEM, and platform-driven automation

Providers	HFS point of view
Hexaware	Delivering cloud-first cybersecurity with zero trust, AI-driven threat response, and compliance-centric delivery
Hitachi Cyber	Advancing IT-OT converged cybersecurity with AI-driven threat defense, global operations, and certified resilience
IBM	Transforming enterprise cybersecurity through AI-driven, data-centric solutions that secure hybrid cloud, identities, and quantum-era threats at scale
Infosys	Delivers integrated cybersecurity across threat exposure management, AI-enabled detection, and industry-specific transformation programs
LTIMindtree	Delivers engineering-led cybersecurity with zero trust foundations, threat management, and automation-first delivery
Mphasis	Offers digital-first cybersecurity with cloud-native detection, DevSecOps alignment, and scalable response models
NTT Data	Driving zero trust and AI-driven cybersecurity with global delivery, platform innovation, and vertical depth
Orange Cyberdefense	Intelligence-led, threat-focused cybersecurity with European roots, global reach, and proven outcomes
TCS	Secures enterprise transformation with consulting-led threat modeling, identity protection, and scalable cyber resilience
Tech Mahindra	Delivers experience-led cybersecurity with zero trust frameworks, adaptive protection, and deep telecom security expertise
Unisys	Delivers secure-by-design outcomes with AI-driven threat detection and deep zero-trust capabilities
Wipro	Delivers end-to-end cybersecurity with OT threat management, intelligent automation, and strong ecosystem collaboration

Note: All service providers are listed alphabetically.

# HFS Horizons for Cybersecurity service providers, 2025



Note: All service providers within a Horizon are listed alphabetically.  
Source: HFS Research, 2025

Horizon 3 service providers demonstrate

- Horizon 2 +
- The ability to drive the ‘OneEcosystem’ approach to enable a comprehensive, predictive security posture.
- The ability to help enterprises seamlessly adapt to dynamic business needs and evolving threat landscapes.
- Enabling continuous innovation to help enterprises stay at the forefront of technology and transformation.
- Well-rounded capabilities across all value creation levers: talent, domain, technology, data, and change.
- Driving co-creation with clients and ecosystem partners.

Horizon 2 service providers demonstrate

- Horizon 1 +
- The ability to drive the ‘OneOffice’ mindset to break down the barriers imposed by the value chain.
- The ability to enable contextual, adaptable security posture through strong domain capabilities.
- Global capabilities with strong consulting skills and partnerships with major hyper-scalers.
- Capabilities to deliver end-to-end transformation with ongoing multi-year managed services.
- Clear articulation of the operating model.
- Proven and leading-edge proprietary assets, including different platforms.


Horizon 1 service providers demonstrate

- The ability to support security enhancement of digital estates.
- The ability to reduce the costs of cybersecurity delivery with a relevant set of offerings.
- Robust fundamentals of innovation and transformation.
- Referenceable and satisfied clients for the ability to execute cybersecurity resilience.

# 4

## EY profile: Cybersecurity services, 2025

# EY: Drives board-level cyber alignment through GRC, AI assurance, and consulting-first delivery models

<div> <div>HORIZON 3 – Market Leader</div> <div>  </div> <div>HORIZON 2 – Enterprise Innovator</div> <div>HORIZON 1 – Disruptor</div> </div>	<div>Strengths</div> <ul style="list-style-type: none"> <li> <b>Value proposition:</b> Positions cybersecurity as a catalyst for enterprise value, blending sector-led insights, lifecycle-based delivery, and a co-sourcing model to help clients become ‘secure creators’ that transform cyber risk into growth, resilience, and trust.         </li> <li> <b>Capabilities:</b> Offers an end-to-end cybersecurity suite across strategy, advisory, transformation, and operations, anchored in threat detection, identity, risk management, and proprietary assets like EYQ and EY Fabric.         </li> <li> <b>Go-to-market:</b> EY’s sector-led, asset-enabled GTM model integrates 73 cybersecurity centers across 150 countries and 40+ alliances, providing white-glove, globally consistent yet locally tailored delivery.         </li> <li> <b>Outcomes:</b> Delivers measurable results through significant annual savings, operational efficiencies, proactive breach prevention, and regulatory compliance improvements across critical sectors like consumer goods, financial services, and government.         </li> <li> <b>Innovation:</b> Firmwide, EY has invested \$1.7B+ in technology-led innovation, operationalizing GenAI through LLM-powered SOCs, AI-driven threat hunting, and post-quantum cryptography readiness via EY’s Quantum Labs.         </li> <li> <b>Partner:</b> Applaud the brand recognition, consulting expertise, OT/IoT security offerings, focus on customer outcomes, technical capabilities, and commitment to driving innovation, while appreciating their influence with key executives, reliability, and dedication to the partnership.         </li> </ul>	<div>Development opportunities</div> <ul style="list-style-type: none"> <li> <b>Reframe cyber from compliance to resilience enablement:</b> EY could consider evolving from regulatory uplift to embedding cyber as a strategic thread across ERP, supply chain, and OT transformation.         </li> <li> <b>Shape the successor to MSSP through embedded resilience models:</b> EY could explore formalizing its co-sourcing approach into a next-gen managed model that blends advisory, detection, and engineering.         </li> <li> <b>Converge cyber, AI, and data governance into a unified risk spine:</b> As AI risks intersect with data lineage and access controls, EY is well placed to shape integrated governance models across all three.         </li> <li> <b>Partner:</b> Expect increased support from C-suite to C-suite, enhanced lead generation efforts, improved ease of doing business in emerging markets and regions, faster coordination and execution, larger scale, and global coverage.         </li> </ul>
---	--	---

M&A and partnerships	Clients	Global operations and resources	Flagship internal IP
<div>M&amp;A:</div> <ul style="list-style-type: none"> <li> <b>J Group Consulting</b> (March 2025) - Specialized PAM/IAM skills, enhances EY’s market position in Oceania.           </li> <li> <b>Dignari, LLC</b> (Oct. 2024) - Enhances EY’s US public sector cybersecurity offering, particularly in digital identity and access management.           </li> </ul> <div>Key partners:</div> <p>Microsoft, SAP, ServiceNow, CrowdStrike, Saviynt, Zscaler, Splunk, NVIDIA, Dell Technologies, and other regional GTM partnerships.</p>	<div>Number of clients:</div> <p>2,562</p> <div>Key clients:</div> <ul style="list-style-type: none"> <li>A major global snacks brand</li> <li>A global financial services conglomerate</li> <li>A global technology giant</li> <li>A prominent APAC insurance firm</li> <li>A global aerospace giant</li> </ul>	<div>Headcount:</div> <p>18,100+ employees across cybersecurity and IT/tech risk</p> <div>Delivery and innovation locations by major geo:</div> <ul style="list-style-type: none"> <li> <b>73 cybersecurity centers of excellence</b> - 19 in the Americas, 22 in APAC, and 32 in Europe           </li> <li>             Several new cybersecurity service delivery centers have opened in the past 12-24 months, including in Malaga, ESP; Cebu, PHI; and several locations in the Middle East.           </li> </ul>	<ul style="list-style-type: none"> <li> <b>EY Assess</b> – An EY proprietary assessment methodology to measure cyber exposure to risk and provide effective remediation tools leveraging GenAI.           </li> <li> <b>EY.ai Cyber</b> – A suite of AI assets and proprietary accelerators that enhance Cyber offerings with AI/LLM capabilities, supporting methods development and client engagements.           </li> <li> <b>EY PARIS</b> – A privileged access management tool with built-in rules and criteria for privilege identification, offering automated account discovery, scans, and reporting for clients.           </li> <li> <b>EY Cyber Operations Platform</b> – A proprietary platform for delivering operated/managed security services offerings.           </li> </ul>

# 5

## HFS Research authors

## HFS Research authors (1/2)

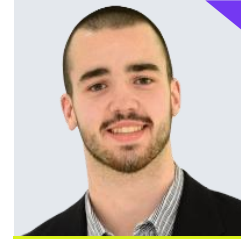


**Akshat Tyagi**  
Associate Practice Leader  
[akshat.tyagi@hfsresearch.com](mailto:akshat.tyagi@hfsresearch.com)

Akshat Tyagi is an Associate Practice Leader at HFS Research, specializing in cybersecurity and emerging technologies such as Web3, blockchain, and quantum computing.

He brings over eight years of experience as a research analyst at Protiviti, Gartner, and EY, advising C-suite leaders on cybersecurity strategies. His work tackles critical business challenges such as securing AI-driven ecosystems, ensuring regulatory compliance, and balancing innovation with risk management. Akshat has also supported global organizations in establishing and scaling their global capability centres (GCC) in India, guiding security, compliance, and operational complexities.

Akshat's expertise covers enterprise security architecture, IAM, threat detection and response, and cloud security. He focuses on integrating automation, behavioral analytics, and threat intelligence to enhance enterprise security resilience. He also actively researches the evolving role of frontier technologies in shaping cybersecurity, governance, and digital transformation.



**Jason Dann**  
Research Analyst  
[jason.dann@hfsresearch.com](mailto:jason.dann@hfsresearch.com)

Jason Dann is a Research Analyst at HFS Research and is based in Boston, MA. He focuses on the evolving landscape of sports technology and the broader services ecosystem that supports enterprise transformation. His work spans multiple industries, with a particular emphasis on how service providers enable organizations to meet their strategic objectives.

Jason leads HFS's research in the Sports & Entertainment space, drawing on his background as a former college athlete and deep interest in the intersection of sports and technology. He is especially focused on how innovation is enhancing operational performance and delivering superior experiences for both sports organizations and their fans.

## HFS Research authors (2/2)



**Ashwin Venkatesan**

Executive Research Leader

[ashwin.venkatesan@hfsresearch.com](mailto:ashwin.venkatesan@hfsresearch.com)

Ashwin is an Executive Research Leader at HFS Research. He has over 18 years of experience in the global business services (GBS) and technology services advisory space and a proven track record as a trusted advisor for C-level executives and services leaders across Fortune 2000 enterprises and service providers.

Before joining HFS, Ashwin was a director at Deloitte's GBS consulting practice, where he spearheaded consulting engagements to help clients set up, scale, and mature their global capability centers and outsourcing portfolios. He was involved in multiple initiatives covering the GBS lifecycle (strategy, design, and implementation/continuous improvement) across tech/digital, ER&D, and business operations.

He also held positions at Everest Group (incubating the Cloud and Infrastructure Services analyst and advisor practice and developing advisory offerings for enterprise IT leaders) and Evalueserve (managing business research teams).



**Mayank Madhur**

Practice Leader

[mayank.madhur@hfsresearch.com](mailto:mayank.madhur@hfsresearch.com)

Mayank Madhur is a Practice Leader at HFS Research, driving deep research and insights into the healthcare and life sciences verticals. He also brings horizontal depth in IoT, digital engineering, and sustainability, collaborating with industry and technology leaders to deliver cross-functional insights. He holds the Sustainability and Climate Risk (SCR) certification from GARP and is a certified Project Management Professional (PMP®).

With over a decade of experience in research, strategy, pre-sales, and software development, Mayank blends analytical rigor with execution. At Altimetrik, he supported vertical heads and GTM teams, contributing to M&A profiling and peer benchmarking. At HCLTech, he worked on an R&D project for a global medical device client.

He holds an MBA from BITS Pilani and a bachelor's degree in electrical and electronics engineering from VTU. He also completed an executive program in strategic management from IIM Kashipur and a postgraduate diploma in public health. He is currently pursuing a PGPM in healthcare from LIBA and a doctorate in management studies focused on India's healthcare ecosystem.



## About HFS

- **INNOVATIVE**
- **INTREPID**
- **BOLD**

HFS Research is a leading global research and advisory firm helping Fortune 500 companies through IT and business transformation with bold insights and actionable strategies.

With an unmatched platform to reach, advise, and influence Global 2000 executives, we empower organizations to make decisive technology and service choices. Backed by fearless research and an impartial outside perspective, our insights give you the edge to stay ahead.



[www.hfsresearch.com](http://www.hfsresearch.com)



[hfsresearch](https://www.linkedin.com/company/hfsresearch)



[www.horsesforsources.com](http://www.horsesforsources.com)



[www.horsesmouthpodcast.com](http://www.horsesmouthpodcast.com)