OMDIA UNIVERSE

Publication date:
12 Jun 2024

Author(s):
Adam Etherington, Senior Principal Analyst, Digital Enterprise Services

Omdia Universe: Global IT Security Services Providers, 2024

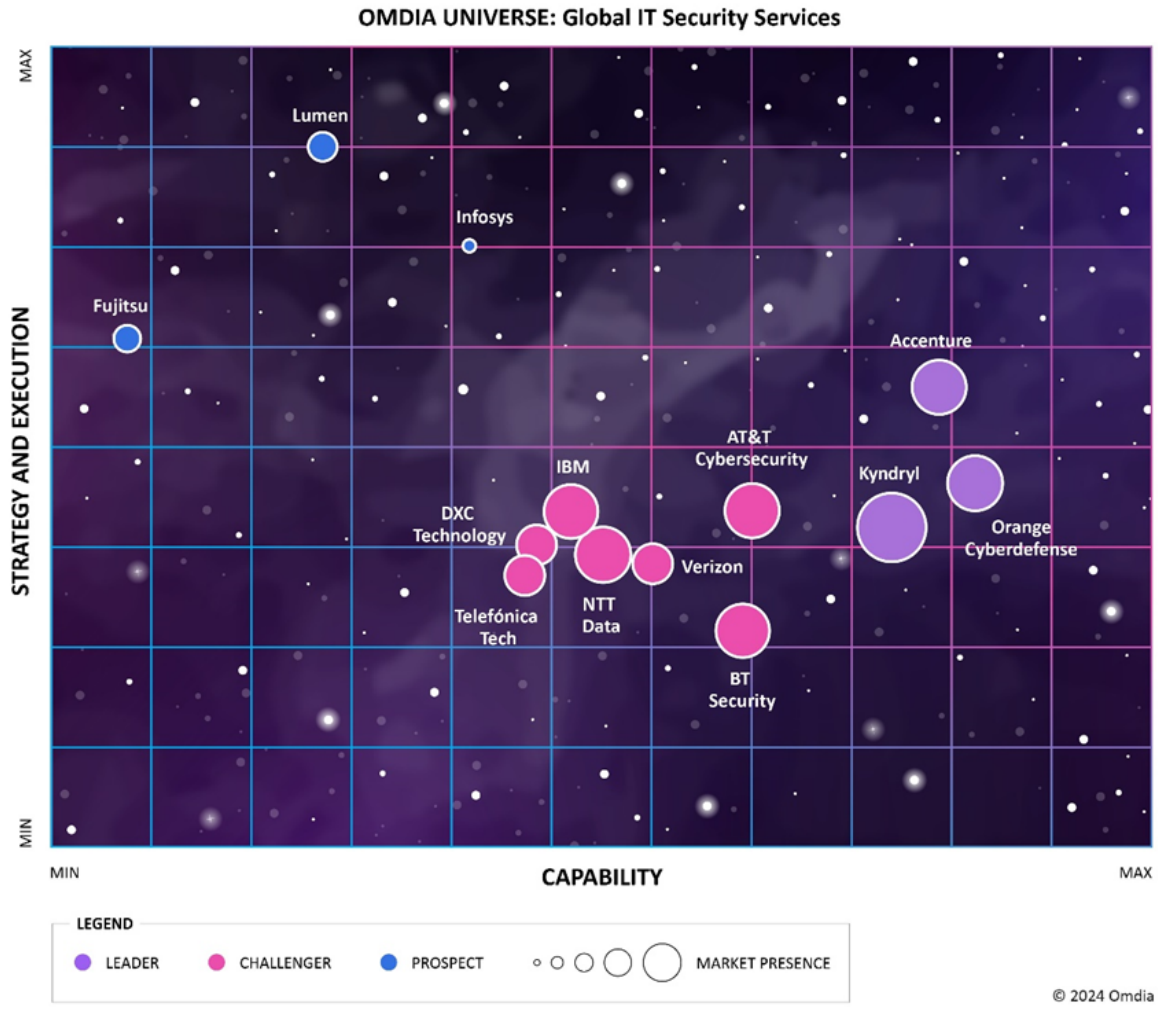
Brought to you by Informa Tech

Summary

Catalyst

This Omdia Universe offers an independent, comprehensive assessment of leading global IT security service providers across two significant dimensions: overall customer & service experience capability and end-to-end global IT security services solution capability. The overall Omdia Universe result is shown in **Figure 1**.

Figure 1: The Omdia Universe for Global IT Security Services Providers



Source: Omdia

The comprehensive benchmarking conducted in this report assessed the full breadth of in-market IT security services across five main categories, which are the foundation of any modern large enterprise and government organization:

- Managed security services (MSS).
- Consulting and professional security services.

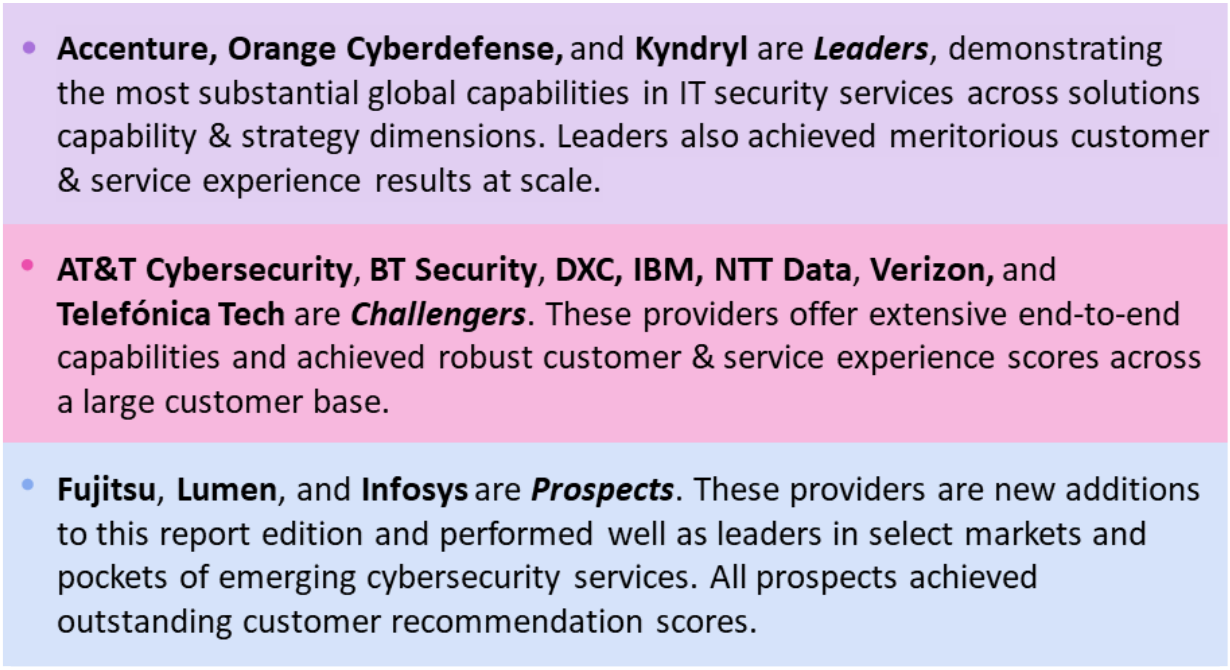
- Innovative and emerging security services.
- Industry cybersecurity solutions.
- Cybersecurity technology and software.

We trust that this Universe will assist any CIO, CTO, chief information security officer (CISO), procurement, or other senior decision-makers at large multinational corporations (MNCs), enterprises, or government agencies responsible for shortlisting IT security services providers.

Omdia view

Figure 2 shows the vendors covered in this 2024 updated edition of the Omdia Universe for Global IT Security Services.

Figure 2: Vendor rankings in the Global IT Security Services Providers Universe



Source: Omdia

Market definition—IT security (cybersecurity) services providers

Throughout this report, IT services and cybersecurity refer interchangeably to service-based solutions that help organizations address the confidentiality, integrity, and availability of information and communications systems.

The market for IT security services is relatively mature and complex. Omdia notes that the service providers assessed in this report frequently use different terms for comparable services. For consistency and comparison to capture the most critical, holistic IT security services, Omdia defines five categories in this Omdia Universe (refer to **Table 1** for a summary of the taxonomy).

For a deeper evaluation, Omdia groups these five service areas into two capability categories, which are part of each Vendor Radar Chart:

- **Core Services** provides the foundational IT security services required by large enterprises and government agencies. These include managed security services, professional security services, consulting, and value-added resale.
- **Extended Services**—more specifically, tailored or innovative IT security service offerings—including emerging capabilities and industry-specific security solutions.

Table 1 offers more details of the components in each solution group.

Table 1: Market Definitions—Omdia Universe IT Security Services Providers

Core services: • **Managed security services (MSS):** 24×7×265 security operations, incident monitoring, investigation, and response services under an annuity or retainer outsourcing arrangement with organizations from central and regional security operations centers (SOCs). MSS broadly includes managed detection and response (MDR), threat detection and incident response (TDIR), managed SIEM and SOC, advanced SOC service, and similar variants. • **Professional services & consulting (PS&C):** Security-specific professional services, advisory, consulting expertise, and skilled labor to perform assessment, strategy, design, implementation, and optimization services across multiple security domains (e.g., cloud, networks). Examples include CISO advisory, penetration & vulnerability testing, staff security awareness training, and ad-hoc emergency incident response. • **IT Security technology and services (including value-added resale).** Providers are a valuable and necessary volume- and value-based channel that pulls together the extensive and highly fragmented cybersecurity platform ecosystem. Leading vendors such as Microsoft, Palo Alto Networks, Cisco, AT&T, CrowdStrike, Nozomi, and Sophos depend on partners for market reach, expertise, customer access, and ongoing service delivery with their platforms across software, appliances, and cloud-based deployments.
Extended services: • **Innovative and emerging security services.** A new category in this Omdia Universe edition, providers invest in deep domain capabilities with customers, partners, industry bodies, and institutions to deliver cutting-edge IT security capabilities as a service. Prevalent examples include secure access service edge (SASE), MDR, AI/ML, IoT/Industrial Internet of Things (IIoT) service capabilities, or outcome-based SLAs as non-bespoke, repeatable service offerings. • **Industry cybersecurity services.** Includes sector-specific combinations of MSS, PS&C, innovative solutions, and value-added resale to meet unique regulatory requirements and industry standards. These services are usually delivered as an overlay, combining horizontal IT security service capabilities with tailored services.

Source: Omdia

Market dynamics

Cybersecurity is increasingly complex and mission-critical. Omdia's research confirms that the volume and severity of cyberattacks continue to increase steadily for large organizations across all major sectors, necessitating increased security spending for over 40% of firms globally, with far-reaching impacts.

From extensive primary research, the imperatives that security leaders must address include:

- **Security incidents frequently cause expensive downtime.** In the past 12 months, 35% of firms told Omdia they suffered operational downtime due to a critical incident or breach. These impacts are potentially devastating. Most firms saw a cluster of negative consequences, including decreasing profitability, increased security spending, and increased management scrutiny from regulators and the boardroom.
- **The severe financial impacts of a major incident & breach**. Across the 212 firms that Omdia surveyed in 2024, organizations hit by a significant incident or worse on average lost an estimated 20% of revenue and saw profitability reduced by 15% across the affected period. The severity of the impact varied across industries. So, too, did the likelihood of impact. To understand the latest attacks and risks, firms should assess vendor and provider thought leadership on threat analysis across attack vendors and effects.
- **Service providers help address critical security capabilities for large firms.** The service providers assessed in this report bring expertise and scale to address complex cyber challenges. The top three areas CISOs consider their organizations to be the least prepared—where they need help most—are expertise in consolidating and integrating security tools, addressing IT and operational technology (OT) security convergence, and leveraging emerging technologies and platforms (e.g., AI, extended detection and response (XDR), and SASE).
- **Choosing the right provider.** While every firm is ultimately responsible for its cyberdefense, risk, and compliance, the degree to which each organization engages third parties differs considerably. Leading providers offer consulting, advisory, and managed services. They also offer emergency incident response services across IT and now OT environments. Providers can use their breadth of expertise to serve a range of complex enterprise environments. However, most providers find managed services product lines the most profitable and invest accordingly.

Market outlook: Global IT security services

Driven by rising threats and increasing dependence on digital technologies, Omdia forecasts that the total addressable market for all dedicated IT Security Services will reach ~$130bn in 2028, growing at 10.7% CAGR (2024–28)

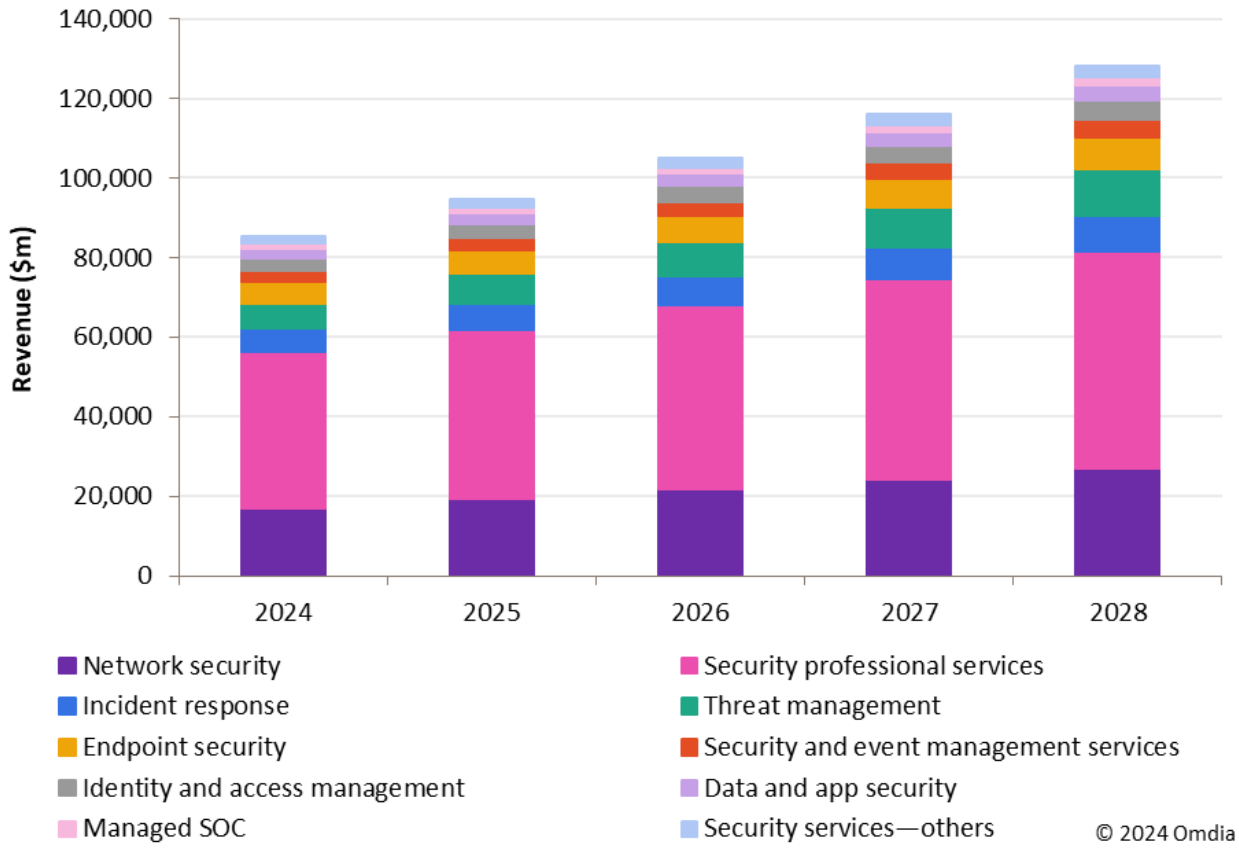
Security represents approximately five percent of all IT services, but it is one of the fastest-growing segments. In global surveys, IT and business executives rank it as a top priority due to the cost of disruption from a significant security incident, breach, or government or legal intervention.

Within security service categories, managed security (including MDR) and emerging security services (including SASE, OT security, and AI-infused solutions) are presently the fastest-growing categories. While tight monetary conditions have temporarily slowed down many large-scale consulting and professional

services engagements, firms continue to innovate with digital technologies, where protection through cybersecurity is a critical element.

Over time, Omdia anticipates that privacy, governance, risk, and compliance will gradually have a greater influence over their choice of security service providers. More mature enterprises are shifting from the "what" and "how" of implementing security to the "so what" and impact of inevitable attacks or, worse, a breach.

Figure 3: Global IT Security Services Forecast, 2024–28 ($m)

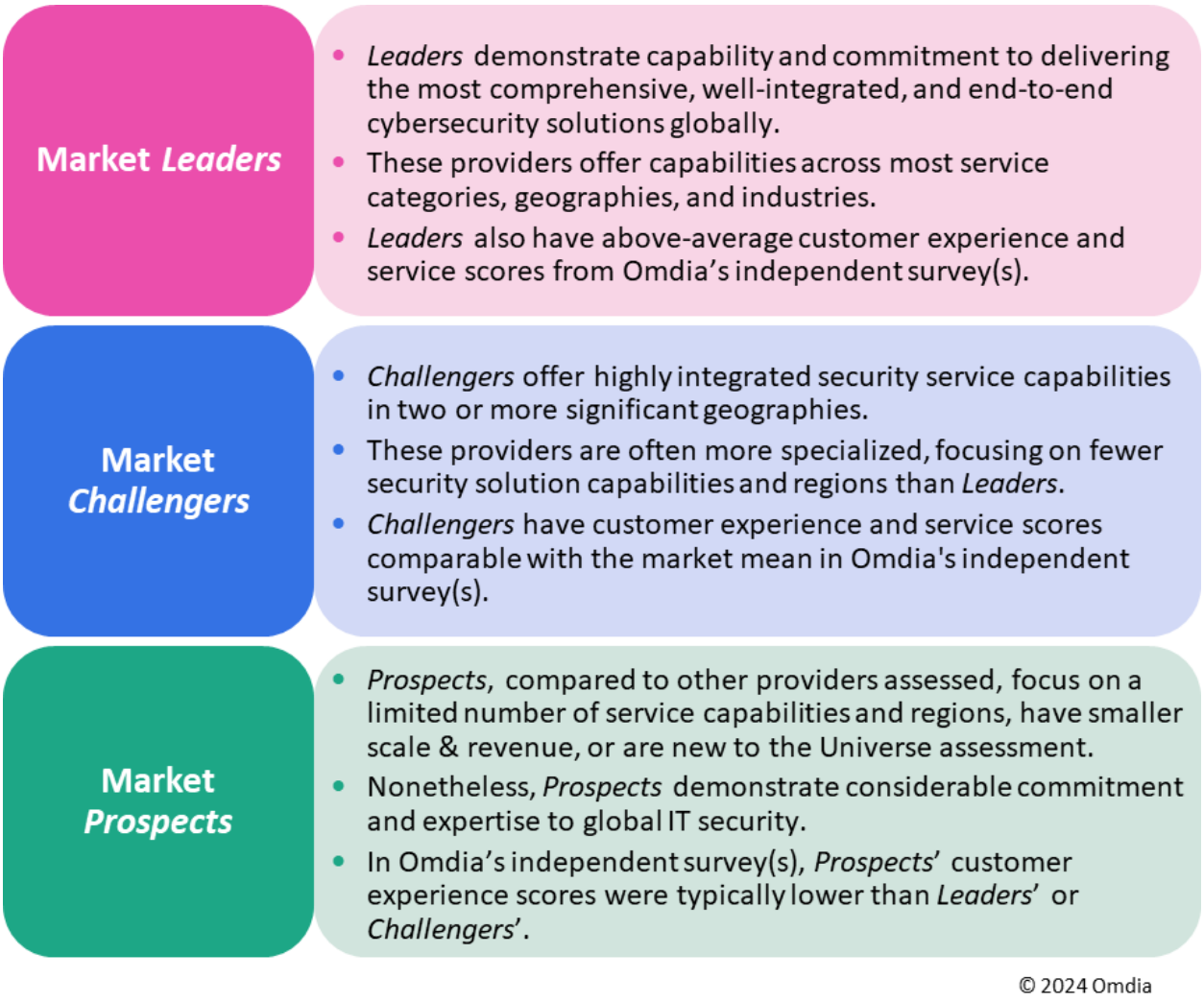


Source: Omdia

Global IT security services, 2024 categories

All providers included in this report have met a high benchmark for inclusion criteria. The following ranking categories tier providers based on multiple service and customer dimensions.

Figure 4: Omdia Universe Global IT Security Services Categories



Source: Omdia

Established versus emerging providers

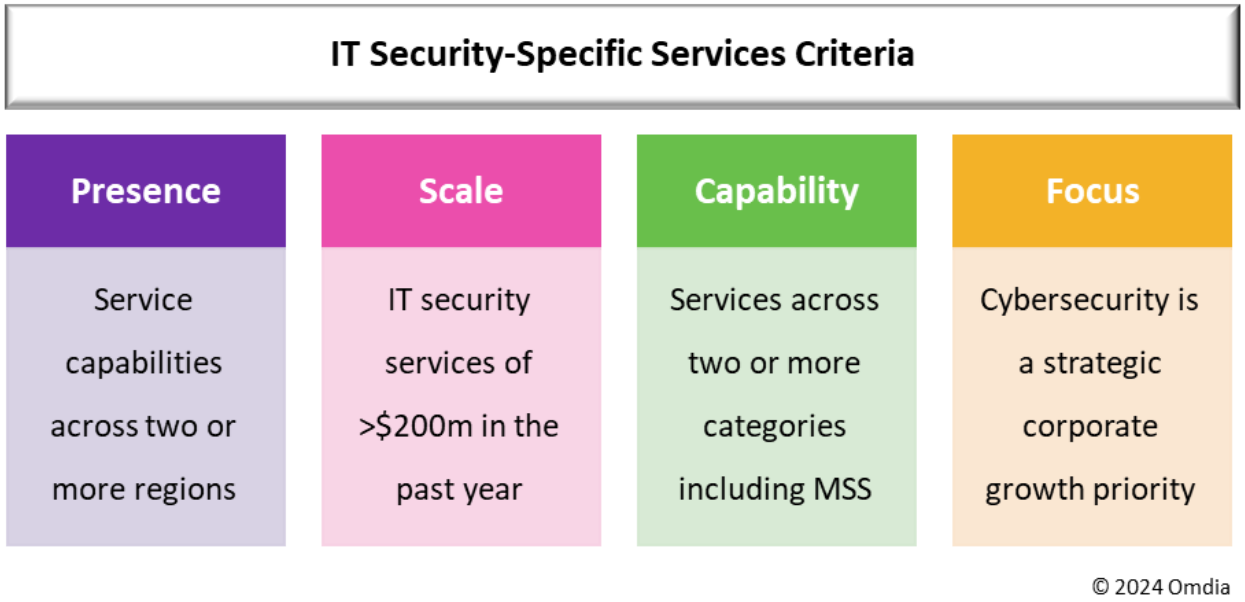
To delineate the findings of this report, Omdia categorizes all service providers based on their inclusion in prior editions and scale:

- **Established Providers:** This survey benchmarks IT security service providers, including Accenture, AT&T Cybersecurity, BT Security, DXC Technology, Orange Cyberdefense, IBM, Kyndryl, NTT Data, Telefónica Tech, and Verizon Business.
- **Emerging Providers:** This report includes Fujitsu (Global), Lumen, and Infosys. This category contains providers with less security-specific revenue than the group median or the providers new to this benchmark assessment.
- **All Providers:** Includes both established and emerging providers (i.e., all providers evaluated met *the inclusion criteria).*

Omdia Universe scope and methodology

The Omdia Universe for Global IT Security Services requires service providers to meet the following benchmark inclusion criteria.

Figure 5: 2024 Omdia IT Security Services Universe—High-level inclusion criteria



Source: Omdia

Universe ratings and scoring

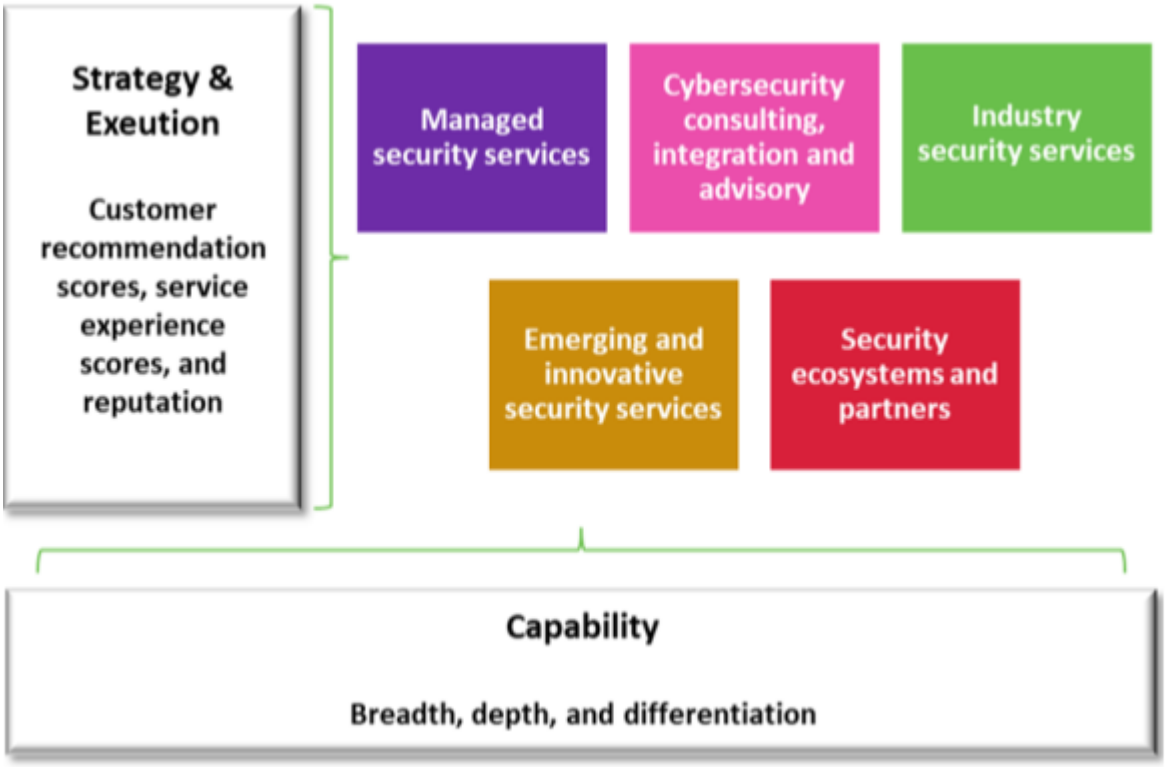
As **Figure 1** illustrates, the overall Omdia Universe ratings reflect scores across the overall Strategy and Execution (Y-axis) and Capability (X-axis).

Scoring includes customers' net recommendation and service experience scores from an independent, Omdia-commissioned primary proprietary research survey of more than 200 senior decision-makers at large enterprises, conducted in 1Q24.

All respondents had direct experience with one or more service providers. They provided direct scores on “likelihood to recommend” and “security service(s) experience” from their provider(s) in the past 12 months.

This report's benchmarking also draws on provider responses, Omdia analyst assessments from publicly available information, and service provider analyst briefings.

Figure 6: Omdia Universe scoring—IT security services



Source: Omdia

Omdia invited all providers in this report to participate through a request for information (RFI) and briefing process.

This report can guide, inform, and expedite a selection process for end-user organization decision-makers to match provider capability to MNCs, enterprises, and governments.

For service providers, this report highlights opportunities and market perceptions to consider in cybersecurity roadmaps, customer advocacy, partnering, product management, and market positioning.

Provider analysis

Accenture (Omdia recommendation: Leader)

Accenture should appear on your shortlist if you are a large enterprise with a complex ICT and digital transformation agenda that requires embedded security services

Accenture continues to focus on large-scale, complete technology solutions, of which cybersecurity is an important capability. Omdia recommends large enterprises consider Accenture for security consulting and management services embedded in large-scale, digital transformation projects across cloud, AI, and enterprise application modernization & management.

In Omdia's direct survey of Accenture customers, Accenture is the leading consulting, integration, and advisory services provider, ranking first with a +56 net recommendation. Accenture's service experience score was 6.97 out of 10, ranking fourth amongst established providers and sixth overall.

Figure 7: Omdia Universe ratings—Accenture

Source: Omdia

Strengths

Broad capabilities in complex ICT and C-suite level thought leadership and access

Accenture is in a prime position to embed security and resilience as part of enterprise-wide digital transformation, enterprise application migration, management, and optimization solutions. M&A in data and AI complements prior cloud investments.

Security capabilities within Accenture's technology services division directly benefit from the company's other service divisions, and the strategy and consulting divisions provide access to C-suite executives. The provider brings a unique capability to address many moving parts across people, process, technology, and change, serving standalone projects and ongoing managed services.

Accenture historically has access to senior executive decision-makers and influencers because of its global scale, breadth of capability, and brand. In cyber, the provider has pivoted its thought leadership emphasis from threat intelligence to address C-suite concerns, including "The Cyber-Resilient CEO" and "State of Cybersecurity Resilience," accompanied by senior practitioner-written blogs. Not all providers have the credibility or insight to write directly to this level of the audience with a broad perspective.

Limitations

Communicate a clear, standalone cybersecurity strategy and improve industry cybersecurity customer experience

Accenture must clarify its global, end-to-end cybersecurity services strategy that ties together aggressive M&A with patents and service evolutions, for example, from managed security services to cybersecurity delivered as a service, partnerships, and customer messaging. Accenture also needs to articulate how it is a security-focused partner—aside from larger-scale digital programs—to help CISOs develop and mobilize complex cybersecurity programs.

Accenture's recommendation and organizational experience scores for industry- and sector-tailored-specific security services were below those of prior surveys and other providers. Given the provider's presence in all major sectors and breadth of experience, addressing the service delivery or expectation gap reflected in its service experience scores should be a priority.

AT&T Cybersecurity (Omdia recommendation: Challenger)

AT&T Cybersecurity should appear on your shortlist if your enterprise needs global reach and a standardized approach

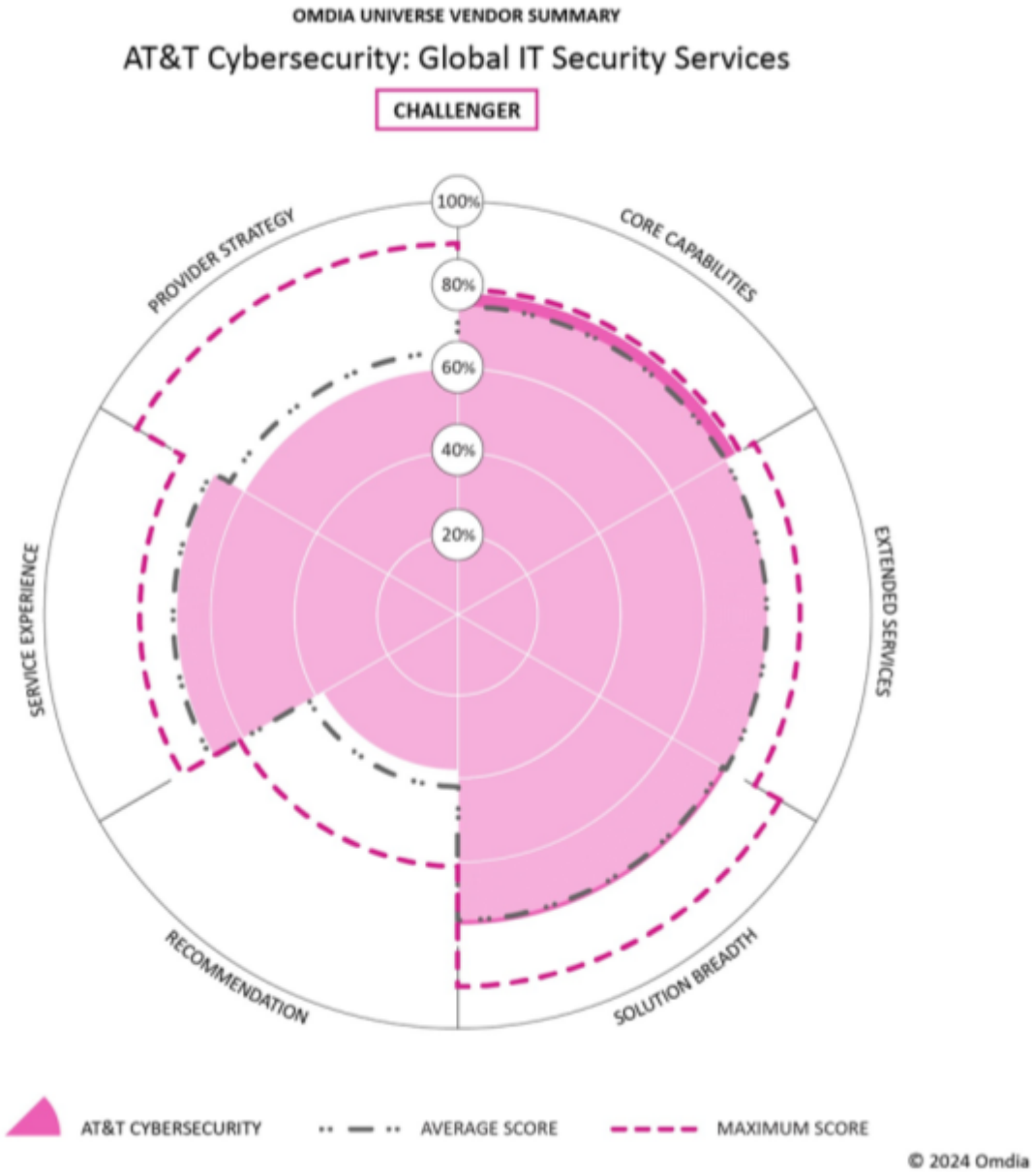
Overview

AT&T Cybersecurity was the standalone IT security division for AT&T Business and an established global provider of IT security solutions. In late 2023, the cybersecurity division announced plans to become a joint venture with Chicago-based investment firm WillJam Ventures. The new entity, LevelBlue, offers a broad cybersecurity services portfolio spanning cybersecurity consulting, managed networks, security operations services, and research.

In this Universe edition, Omdia assessed AT&T Cybersecurity based on capabilities, strategy, and reputation prior to the LevelBlue announcement. Overall, the provider achieved a weighted recommendation score of +35, ranking sixth among established players.

AT&T Cybersecurity achieved a Challenger ranking based on the customer experience and service experience scores, combined with reputational considerations from corporate announcements and the forthcoming JV with WillJam Ventures.

Figure 8: Omdia Universe ratings—AT&T Cybersecurity



Source: Omdia

Strengths

Global scale and breadth with a robust channel and thought leadership

AT&T Cybersecurity offers excellent service breadth across consulting, network, MDR/XDR, and endpoint management. Capabilities are integrated and repeatable for customers as the provider and its partners leverage the proprietary AT&T Cybersecurity USM Anywhere (now LevelBlue USM Anywhere under the new brand), an open XDR-enabled platform for integrated threat intelligence. The USM Anywhere platform has been certified for SOC II Type 2, PCI/DSS, ISO 27001, ISO 27701, and HIPAA.

The provider has over 1,300 security specialists and supports clients through eight Global SOCs in North America—including an MDR-specific SOC—Europe, and Asia & Oceania. AT&T has security/network

operations centers that include hardened facilities for government and private contracts, including staff with government clearances.

AT&T Cybersecurity has achieved considerable growth from its indirect channel. The provider delivers threat intelligence enriched by its Alien Labs R&D center and collaboration with the Open Threat Exchange (OTX).

The providers' leading sector-specific cybersecurity offerings continue to evolve. AT&T Cybersecurity has defined important network and industry-nuanced security considerations across critical sectors, including manufacturing, BFSI, healthcare, and retail. Its capabilities in OT security are emerging, with services built on Qualys/Tenable and integrations into USM Anywhere with OT tooling.

AT&T Cybersecurity offers managed solutions from Palo Alto Networks, Fortinet, and Cisco in SASE. In the MDR portfolio, the provider is in generative AI (GenAI) interface capability, advanced query support, and embedded identity management tools. AT&T's MTDR for Gov solution is certified under FedRAMP for US government and commercial entities requiring that certification, and it sits on Amazon Web Services (AWS) GovCloud.

More broadly, the provider's capabilities continue to expand in AI, cyber governance/risk management services, and advancing managed network services, serving greater customer needs.

Limitations

Double down on reputation and presence

AT&T Cybersecurity's overall ranking in this year's report reflects the parent company's customer experience results, ranking, and parent company reputational considerations.

Omdia expects AT&T to achieve deeper market consideration as part of the capital injection and strategic focus afforded by the announced WillJam JV. This move is anticipated to give the provider a degree of autonomy in market differentiation and focus that other providers have experienced from a concerted security focus. A key area to start is in deepening the capability of security consulting and strategy services across its existing MSS large enterprise customer base.

BT Security (Omdia recommendation: Challenger)

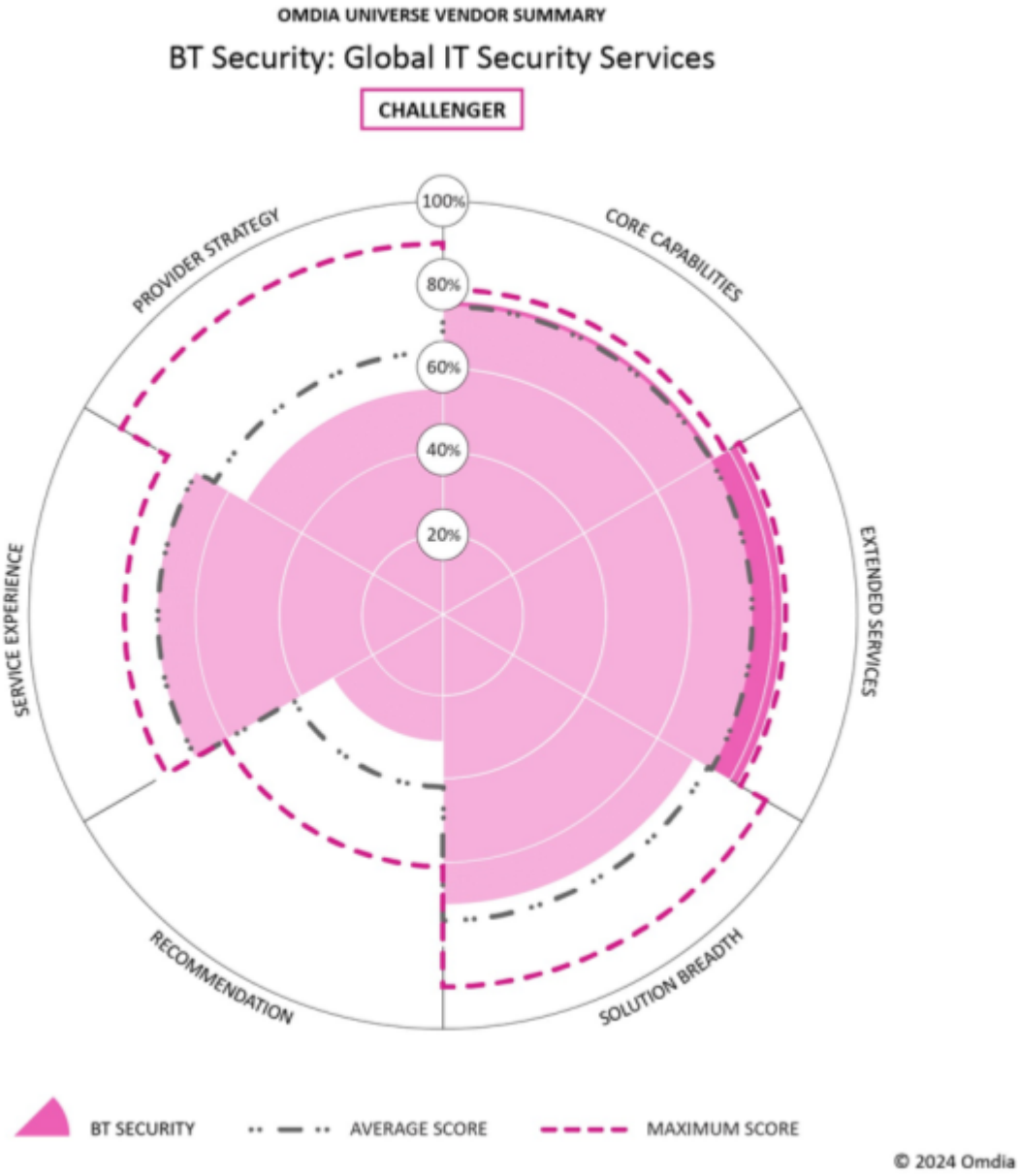
BT should appear on your shortlist if you value a European telco with global managed and advisory security capabilities committed to cyber innovation

Overview

The BT Group Telcos security division is a leader in the United Kingdom market, with the vision of being "the world's most trusted connector of people, machines, and devices." The current security strategy is focused on deepening its core advisory and MSS services to SMBs, the UK government, and MNCs.

BT received an overall customer and service experience score of +32 across global surveyed customers, ranking seventh among established Universe providers. BT achieved a service experience score of 6.76 out of ten, ranking seventh amongst established players. Customers' most positive experiences were in BT bringing together cybersecurity technology software partnerships and delivering emerging services.

Figure 9: Omdia Universe ratings—BT Security



Source: Omdia

Strengths

Leading provider in the mature UK market with security innovation

BT has longstanding experience as a critical infrastructure provider with over 3,600 security professionals delivering advisory services, flexible managed security, and appliances/CPE across all significant IT domains, including the cloud. BT operates 14 SOCs globally and has achieved ISO27001 accreditation.

Additionally, the provider supports the UK National Cyber Security Centre's CyberFirst program. It launched a novel reskilling program, CAPSLOCK, training existing employees for security roles to benefit employees and the industry as skills shortages bite.

Most leading providers have invested in proprietary platforms, and BT is a prime example. BT Group invests over £680m ($869m) annually in security innovation and reports, having achieved over 100 security patents issued annually.

More specifically, BT was a market leader in driving a proprietary platform-supported approach to integrate, analyze, and advise customers based on multiple sources of threat telemetry. BT's Eagle-i automation and orchestration platform links the provider's managed services across the cloud, endpoint, network, data and application, identity, OT, and threat telemetry. Managed services customers of the provider get access to the platform, which assists BT analysts in focusing on the most critical events, with scalable MDR capabilities to automate or semi-automate responses as customers approve. Eagle-i includes pre-built use cases and playbooks that deliver reduced mean time to detect (MTTD) and respond, and that support customers with compliance by offering a complete end-to-end audit trail.

In other innovations, BT is a market leader in facilitating UK-based customer forums, including its successful Customer Advisory Board and Security Advisory Board. The firm's Cyber Assessment Lab (CAL) continually scans the market and looks at new and innovative solutions. The provider also runs extensive research and development programs to help test security technology solutions across 15 market-leading technology providers and maintain relationships with over 100 security vendors and new market entrants. This is a crucial capability as purchased security software solutions continue to expand.

Limitations

Expand channels and partnerships in the Americas and Asia & Oceania

BT Group is sizeable, with a presence in over 180 countries offering connectivity, cloud, and cybersecurity solutions. Omdia notes that companies in mature Western markets are increasingly looking to diversify and grow across regions, which is a growth opportunity. Southeast Asia & Oceania present good ICT growth prospects where BT would profit from more local presence and scale. In the Americas, the BT Federal division is reportedly certified to sell to the US Federal Government. However, the provider's intent and progress in this market is unclear.

The provider should explore indirect and partner-led models in other regions, nested within a more prominent security strategy that leverages its preeminence in the local market for UK and European-based MNCs that want to secure their overseas operations. Key industries should include BFSI, manufacturing, business services, and government, where BT security has demonstrated experience domestically.

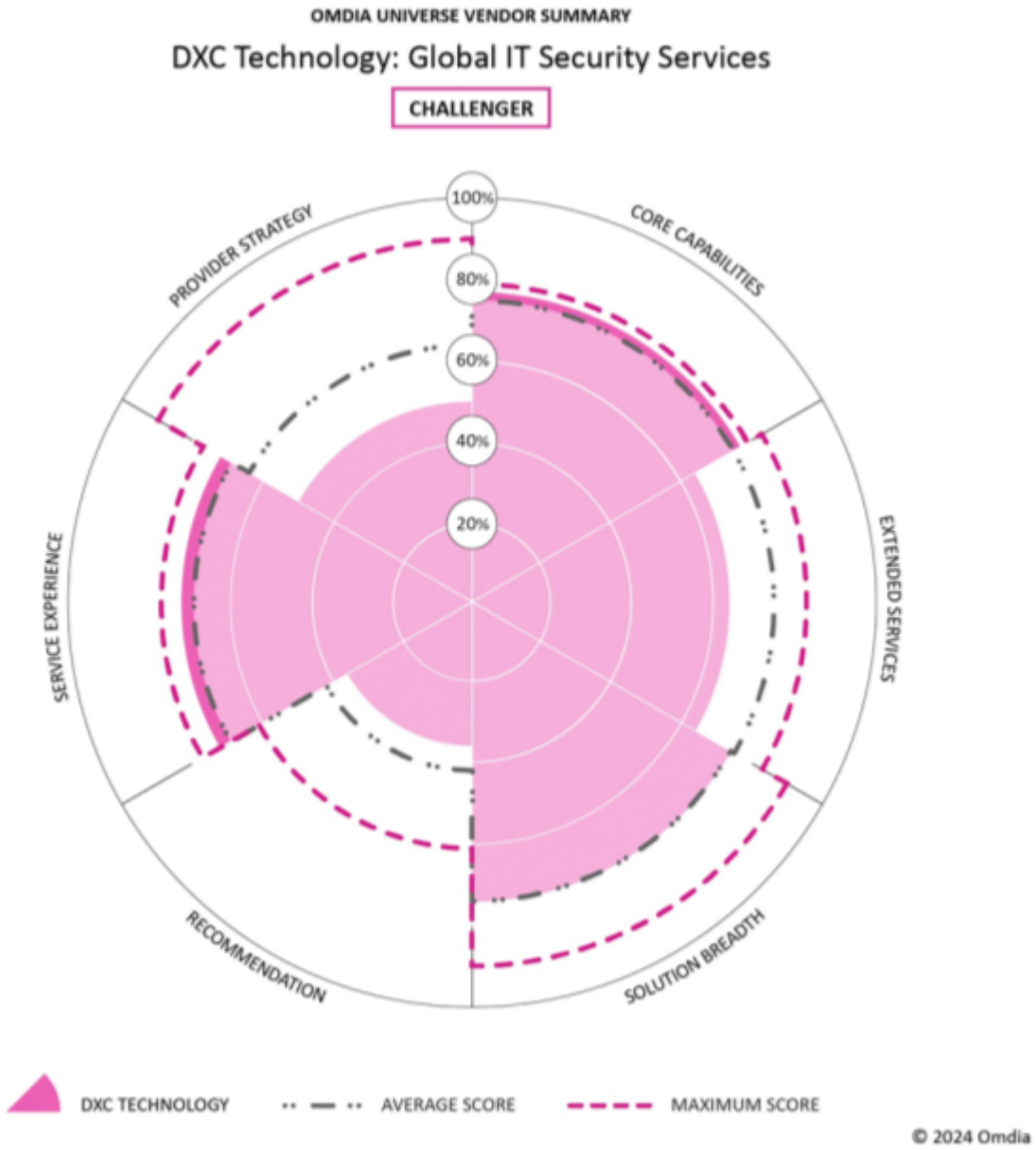
DXC Technology (Omdia recommendation: Challenger)

DXC should appear on your shortlist if your enterprise values an established, experienced, global IT services provider delivering across complex technology environments

DXC is a large systems integrator and outsourcing services company that provides security offerings from its Global Infrastructure Services portfolio. The provider has a global presence spanning major regions and broad service capability, matched with a high degree of security expertise, a deep partner ecosystem, and a high degree of service flexibility under the enterprise technology stack.

In Omdia's direct survey of DXC security service customers, the provider received an overall customer and services experience score of +34, ranking seventh among established Universe peers. The provider received solid marks for service experience in cybersecurity consulting, integration & advisory and high recommendation scores for cybersecurity technology and software services.

Figure 10: Omdia Universe ratings—DXC Technology



Source: Omdia

Strengths

Solid recommendation and service experience scores in consulting and technology

Amongst surveyed customers, DXC scored well in the likelihood to recommend and service experience ratings. The company stood out by achieving the highest overall experience score for cybersecurity consulting, integration, and advisory in this year's benchmark with a +35 net recommendation score.

DXC also achieved the highest score among established firms for integrated cyber technology and software for established firms, with a +20 net recommendation.

Limitations

Asserting a vision and strategy for managed cybersecurity

At the corporate level, DXC has signaled an ongoing commitment to security as a focus area among its portfolio of services, which also include analytics, enterprise applications, cloud & ITO, software engineering, and workplace solutions. However, since the last Omdia Universe benchmark report on global IT cybersecurity services, other past Leaders have surged in capabilities, maturing existing industry innovation and launching new capabilities in managed cybersecurity services. DXC must demonstrate commitment and innovation in this space.

Fujitsu (Omdia recommendation: Prospect)

Fujitsu should appear on your shortlist if you need a globally established provider with expanding regional Asia & Oceania capability, and a global strategy that includes security

Overview

Fujitsu has a heritage as one of Japan's most extensive IT systems and service providers, including security services. The provider has a strategy to achieve growth outside the domestic market, spearheaded by the customer-facing “Uvance” business-focused approach for globally standardized offerings.

As a new provider and prospect in this report, Fujitsu achieved a commendable customer and service experience score of +39 from a smaller base of customers, ranking third amongst newer providers in this year's report.

Figure 11: Omdia Universe ratings—Fujitsu

Source: Omdia

Strengths

Extending robust capability pools from Asia & Oceania, and Europe globally

Fujitsu Global is gathering momentum. The provider now has over 1,200 security professionals, over 500 SOC analysts, and SecOps provided in the Americas (US and Trinidad), Asia & Oceania (Australia, Singapore, and Thailand), Japan, Europe (Finland, Spain, and the UK), and Global Delivery (Poland, India, and the Philippines).

Fujitsu's global portfolio spans security consultancy (e.g., security strategy to technical professional services), threat and vulnerability management (e.g., OT security, SASE), and foundational services across

the NIST framework for cloud, IAM, and other domains. MDR capabilities are also emerging as the provider unites CSIRT, SIEM, and SOAR capabilities across a global network of SOCs.

Fujitsu in Oceania (Australia and New Zealand) has seen exceptional growth through M&A, notably Oobe (government and defense security), InPhySec (specialized security consulting in New Zealand), and MF&A (digital experience and security consulting). The Australian Fujitsu division now has a comprehensive capability set to serve customers across the region and provide a model for global delivery as Fujitsu seeks growth outside Japan.

Limitations

Unifying global capabilities and building a foundational reputation

The global market for end-to-end security services is highly competitive, with providers that offer integrated capabilities across regions.

Historically, Fujitsu has been immense in Japan. More recently, the provider has invested in global capability in Europe, which is now the provider second-largest growth market in security. Fujitsu must articulate a global security strategy for regions and industries, then consolidate capabilities across acquisitions and incumbency to bring a unified and compelling offer that resonates with MNCs.

Security is also a business built on trust. Fujitsu must demonstrate how it leverages security capabilities internally for global group operations and address reputational considerations.

IBM (Omdia recommendation: Challenger)

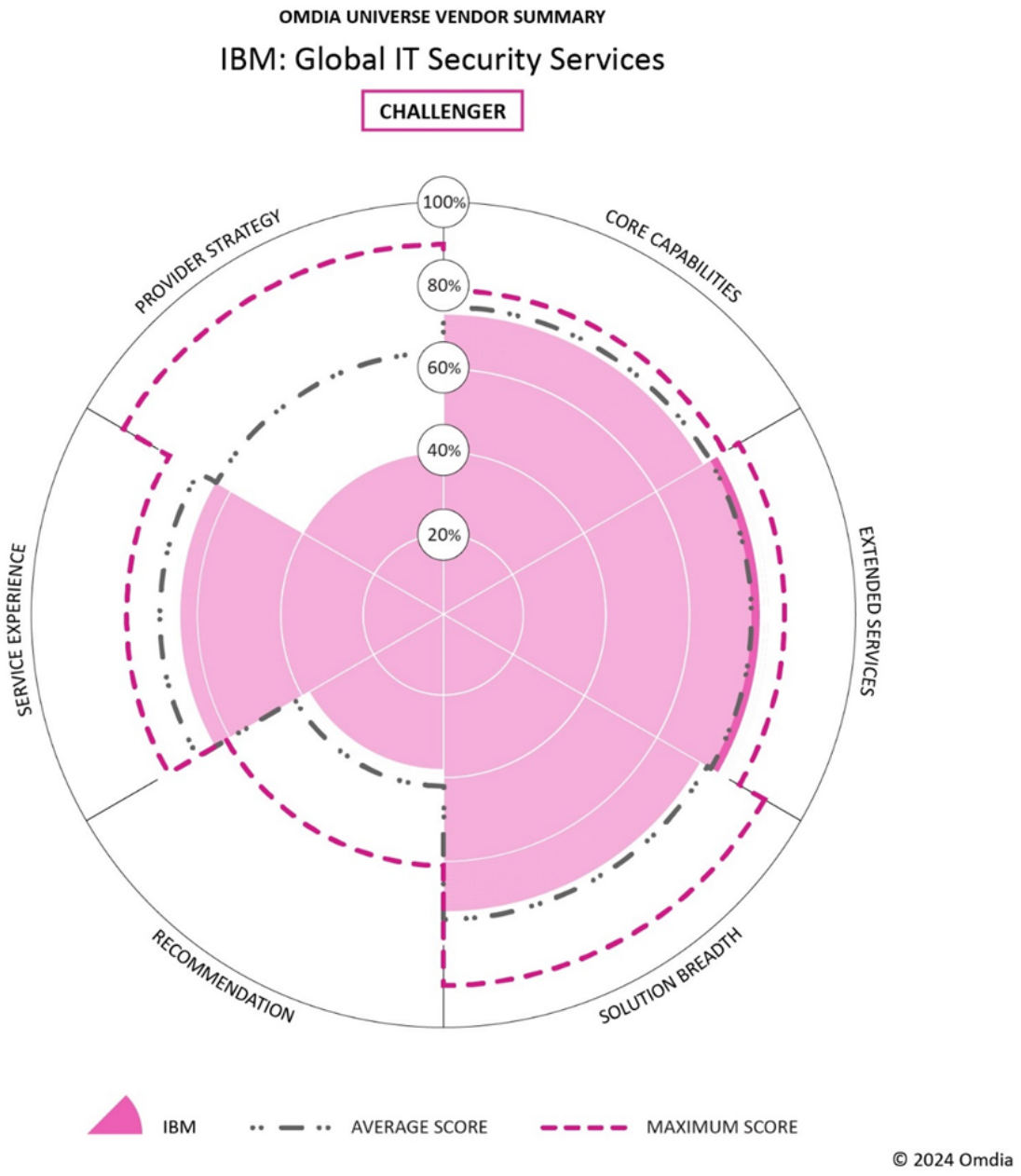
IBM should appear on your shortlist if your organization favors the “Big Blue” ecosystem of platforms, software, and methodologies

IBM remains one of the largest IT service providers in this Omdia Universe. However, there has been a significant strategic shift in security from MSS to focusing on consulting and technology-centric go-to-market services in cloud and AI. Notably, the November 2021 separation of its managed infrastructure services business, rebadged as Kyndryl, and more recently, the sale of IBM's QRadar SaaS assets to Palo Alto Networks and reciprocal services arrangement.

In Omdia’s direct survey of IBM security service customers, the provider received an overall customer and service experience score of +38, ranking fourth amongst established Universe peers. IBM was most likely recommended for managed security services among established firms, with the highest net recommendation score in this category. IBM was also rated well as a consulting partner, with a +32 net recommendation, coming in second among established firms.

IBM's overall service experience score was 6.4 out of 10, ranking it tenth amongst established providers in this highly contested market. Customers rated IBM as the highest in-service delivery standards for cybersecurity technology and software (7.3 out of 10) and industry cybersecurity solutions (6.1 out of 10).

Figure 12: Omdia Universe ratings—IBM



Source: Omdia

Strengths

Market incumbency in security services with deep security platform integrations

IBM retains a sizeable market presence by retaining incumbency in managed security services. The provider continued to deliver to many large organizations post-Kyndyl spin-off with a significant global presence, an extensive network of global SOCs and deep expertise in security platforms and automation, notably Q-Radar. It is understood that the planned PAN partnership will see IBM consulting offer managed security services for legacy IBM and PAN customers migrating from QRadar.

IBM is a leading systems integrator with advanced platforms for hybrid cloud (Redshift) and artificial intelligence (Watsonx). The provider is positioned to work with large and complex clients to address security impacts across an extraordinarily complex ecosystem of ISVs and hyperscalers. In the Omdia direct customer survey, IBM received high net recommendation scores from large enterprise accounts for its consulting and integration.

Omdia's discussion with CISOs confirms that they want to simplify and reduce cost and complexity by consolidating security tools across ICT domains. IBM has historically been well positioned to lead this charge around its security product portfolio, enabled by consulting capabilities, IBM Cloud Paks for security, and deep expertise in X-Force threat intelligence. The new partnership with Palo Alto Networks should improve capabilities in this area, especially as watsonx LLMs are incorporated into PAN Cortex XSIAM to expand AI for cybersecurity capabilities.

Limitations

Receding focus on cybersecurity and smooth custom migrations

Omdia notes that IBM has significantly diminished its messaging, focus, and intent around cybersecurity services as a standalone or strategic business portfolio since 2022. Further, despite being awarded high net recommendation scores, IBM's service experience scores for MSS and emerging services have fallen from prior years.

IBM needs to rapidly clarify its market position, commercial arrangements, and strategy under the partnership with PAN and the impact of the arrangements with Kyndryl. Key areas include how IBM will support large organizations' migration to Cortex XSIAM, their approach to supporting cybersecurity across multiple vendors (non-PAN & QRadar), including what this means for loyal QRadar customers, impacts on security service levels, and joint roadmaps.

Infosys (Omdia recommendation: Prospect)

Infosys should appear on your shortlist for customers wanting a fast-growing global provider with strong platform capabilities

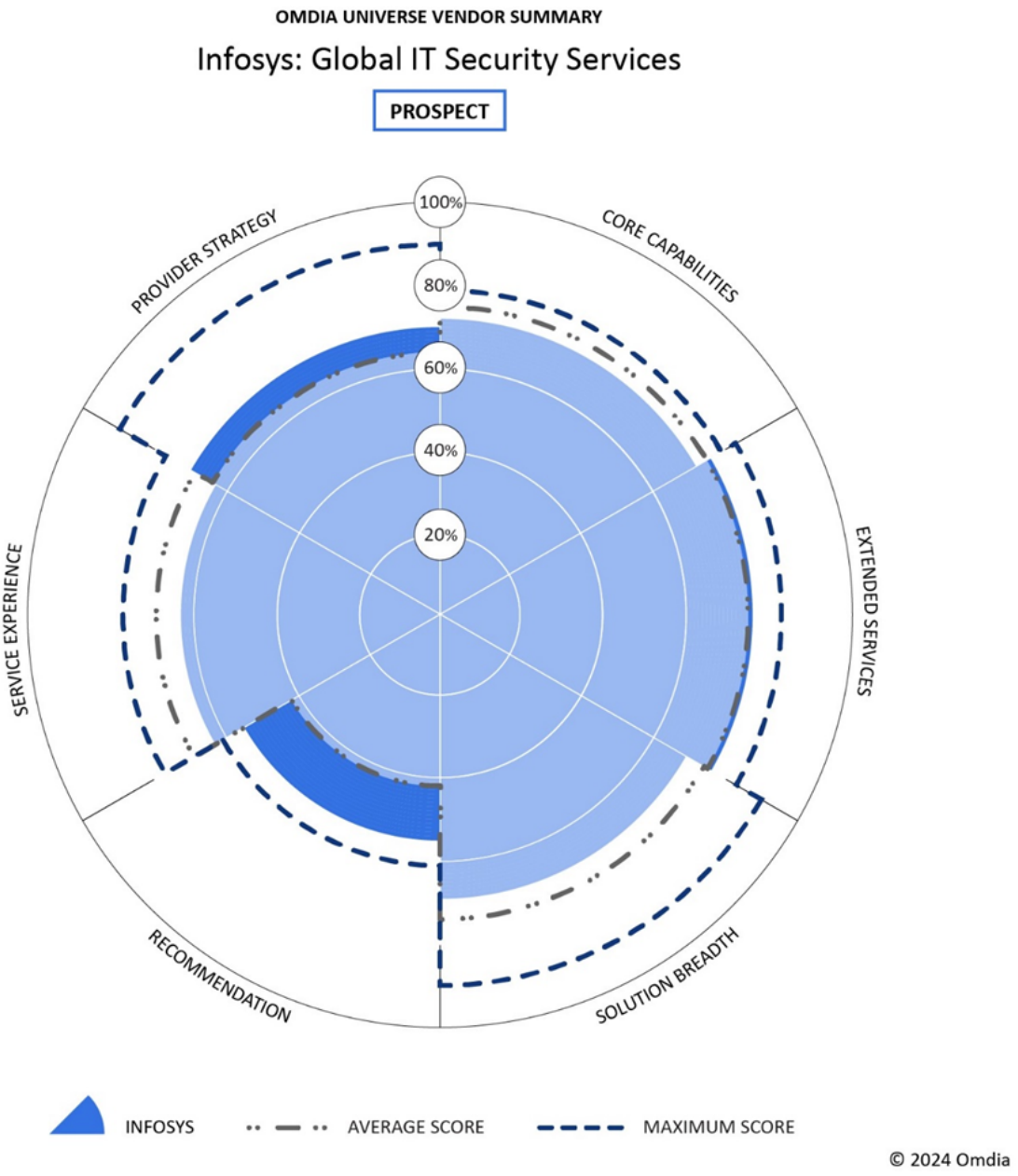
Overview

Infosys is a global provider of digital services and consulting with more than four decades of experience and a presence in more than 56 countries. The provider has established market share in most major sectors, including BFSI, retail, communications, utilities, manufacturing, and healthcare.

Infosys' vision is to, "assure digital trust and cyber resilience at scale to our customers through innovation, service excellence, and competence, and to be the most respected cybersecurity practice globally."

As a new provider and prospect in this report, Infosys achieved an excellent customer and service experience score of +55 from a smaller base of customers, ranking second amongst the newer providers.

Figure 13: Omdia Universe ratings—Infosys



Source: Omdia

Strengths

Comprehensive software-, process- and platform-led approach to complex cybersecurity challenges

Infosys is an experienced systems integrator that has realized rapid growth over the years through IT service management and software engineering.

True to its heritage, the provider has invested in extensive security software, practices, and platform capabilities available to customers. Infosys has been recognized for partner awards from leading Microsoft (e.g., Microsoft Security 20/20 Award for MSSP/TDR Services and 2022 Microsoft Security Modern Endpoint

Management Partner of the Year Award Winner), AWS (Level 1 MSSP), and Zscaler (GSI Growth Partner of the Year).

Infosys offers module-based security that can be delivered standalone and integrated with other offerings. Infosys delivers security services via a global network of eight cyberdefense centers across the US, Europe, and India.

Infosys' Cyber Next Platform Powered Services is core to delivery, comprising six cybersecurity modules, providing security as a service in a single package that combines pre-selected and pre-integrated, ready-to-use security technologies that are partner-supplied or custom-built. These security modules include: "Cyber Watch" (for Security Monitoring & Incident Response with XDR capability for IT & OT environments), "Cyber Intel" (cyber threat intelligence service), "Cyber Hunt" (threat hunting), "Cyber Scan" (vulnerability management) and "Cyber Guard" (managed endpoint detection and response (Managed EDR)). The platform-centric approach plays to Infosys strength in assessing cybersecurity through the elements of a systems integrator.

Limitations

Establishing cybersecurity leadership and thought leadership with a cohesive strategy

Infosys is a relatively new entrant to this Universe assessment and one of the smaller cybersecurity players by revenue. Based on its global presence and expertise in digital transformation, Infosys has assembled an extensive catalog of cybersecurity services. Its capabilities are vast and diffused across many customers in diverse sectors, including mining, utilities, telecoms, retail, and industrial.

As a global SI, Infosys undertakes highly bespoke work across many industries, which would preclude their security services for smaller firms due to minimum, commercially feasible contract size and complexity.

Investments and promoting standardized product offerings across an extensive partner ecosystem, including PAN, Crowdstrike, Microsoft, and Zscaler, will afford the provider a focus on the Fortune 2000 customer base for cybersecurity. Further, Omdia expects Infosys to elevate its standing over time by focusing on a cohesive cybersecurity value proposition for MNCs, continuing to innovate, and leveraging its existing platform-based capabilities and in-house intellectual property with third-party platforms and expertise.

Kyndryl (Omdia recommendation: Leader)

Kyndryl should appear on your shortlist if your organization has complex infrastructure focused on cyber resilience and recovery

Overview

This edition is the first Omdia IT Security Services Universe to include Kyndryl. The provider is not a new entrant: Kyndryl was formed post-spinoff of IBM's Global Technology Services in November 2021. Kyndryl is a Leader in this report, with a robust and focused security strategy, significant scale, and expertise in complex infrastructure security and resiliency.

Kyndryl is heavily invested in cybersecurity, and it has quickly established itself as a leader in managed security services across complex environments in BFSI, healthcare, critical infrastructure, and government. The company brings many notable clients and references from its IBM heritage.

Kyndryl achieved a customer and service experience score of +40, ranking in the top three among established providers. Customers are most complimentary of the provider's MSS capability, awarding a net recommendation score of +17 and a service experience score of 7.38 out of 10, second among established players.

Figure 14: Omdia Universe ratings—Kyndryl

Source: Omdia

Strengths

Rich expertise in complex multi-vendor environments, infrastructure security, and recovery

Kyndryl has more than 7,500 “cyber resilience” practitioners globally who deliver security and recovery services to more than 15,000 client engagements via a combination of global and local/regional SOCs. Kyndryl’s Security & Resiliency practice, including disaster recovery and managed backup, represents 14% of Kyndryl’s $16bn in revenue, or more than $2bn, a large proportion compared to other providers in this survey.

Kyndryl’s strategy is to provide end-to-end security solutions for large organizations through four key domains: security assurance, zero trust, security operations, and cyber incident recovery. Since its 2021 spin from IBM, Kyndryl offers a technology vendor-agnostic perspective to security and resiliency challenges, focusing on bringing the zero trust concept to reality with a customer journey map inspired by subway transit maps. Inspired by subway transit maps, these blueprints enable a real-time assessment of a customer’s maturity across each metro stop.

Consolidation and visibility are challenges across complex technology domains. In this security area, Kyndryl customers can access a single pane of glass via the Kyndyl Bridge Security Operations-as-a-Platform system across MDR, SIEM, and vulnerability services.

Somewhat unique to the market, Kyndryl actively seeks to mitigate “left of boom” threats while implementing disaster recovery processes, tools, automation, and systems to mitigate “right of boom” impacts. Further, Kyndryl has the most substantial focus among Universe peers on cyber resilience, emphasizing the ability to endure and recover from any cyber-led adverse condition, disruption, or compromise that threatens organizations’ critical infrastructure and systems.

Limitations

Expand cloud and risk quantification capabilities, regional coverage, and market positioning

Cloud security is an important area where demand proliferates due to hybrid/multi-cloud environments. Kyndryl's portfolio could call out this area more distinctly, especially for its preventative assessments and consulting capabilities.

Omdia notes that Kyndryl’s visibility of large-scale infrastructure deployment and recovery impacts puts the provider in a frontrunner position to assess the net risk and costs of preventative and managed security services. Kyndryl’s ability to incorporate risk quantification and cost estimates into their customer journey maps gives enterprises a more complete picture for decision-making.

Kyndryl's customer experience and service experience scores indicate that the provider needs to further differentiate its market positioning in security to embrace its heritage while defining its independent future. Investing in regional SOCs across US markets will accelerate this, including the latest Canada SOC formally launched in May 2024. These capabilities will help Kyndryl better serve public sector customers' data localization needs while leveraging global practices.

Lumen (Omdia recommendation: Prospect)

Lumen should appear on the shortlist of organizations and governments seeking a solid North American MSSP with unique threat intelligence

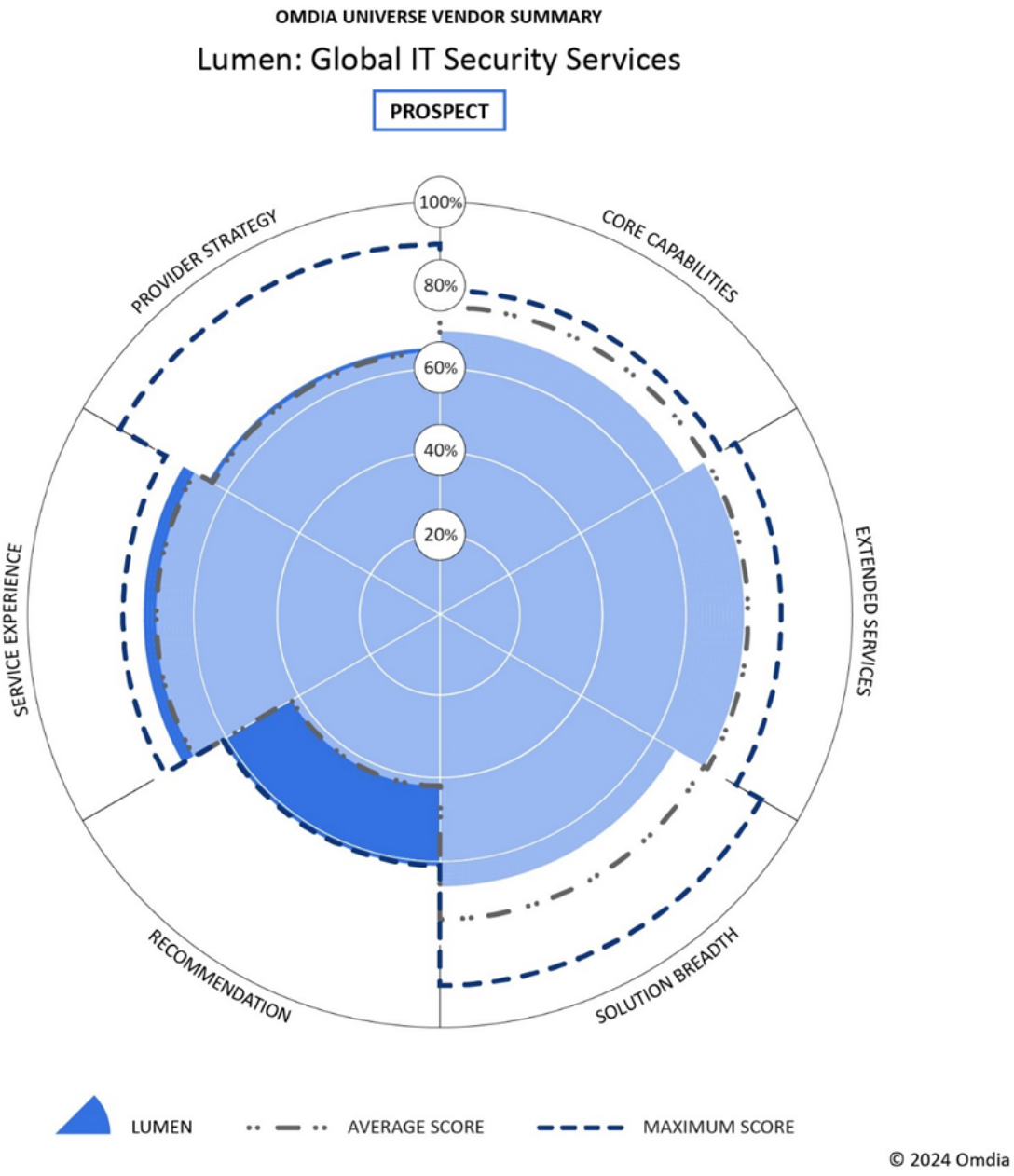
Overview

In this report, Lumen is a leader in North America and a prospect globally. The provider has a specialized security division serving the North American public sector and enterprise clients. It also has a presence in Asia & Oceania and capabilities in Europe and Latin America & the Caribbean through partnership agreements.

The mission of Lumen's security division is to "strengthen every customer's cybersecurity posture leveraging (their) edge/fabric and unique AI/threat intelligence through Black Lotus Labs," which is Lumen's threat intelligence team.

As an established provider and new entrant to this report, Lumen's security division achieved a customer and service experience score of +52, the highest of any provider in this survey. Customers awarded Lumen 7.3 out of 10 for service experience across end-to-end IT security services. Due to Lumen's smaller base in security relative to global peers, these results were from fewer surveyed customers than other providers.

Figure 15: Omdia Universe ratings—Lumen



Source: Omdia

Strengths

Dominance in US MNS and government, emerging global capability

Lumen has an impressive list of US Federal Government clients, with over 1,000 federal customers in over 20 states of the US, serviced by local SOCs and experts. These agreements deliver US federal, state, and local government, as well as education security services. Lumen has a long track record with the public sector, helping clients navigate some of the strictest and most unique security requirements, implementations, and strategies. Lumen's government expertise and capabilities were developed through these partnerships and scaled commercially to serve enterprise customers as productized offers.

Lumen is strongest in secure services edge and managed network security services. Its expertise includes designing, consulting, implementing, and managing network transformation strategies. The provider is a leading provider of SASE offers, including a portfolio of SSE services that include NGFW, ZTNA, SWG, CASB, and DLP, available on-premises and cloud gateways, integrated with core network-based offers. Lumen's SASE on-premises services are available for US-based businesses in over 140 countries globally. Lumen SASE Solutions are available with a choice of service partners: Fortinet and, as of April 2023, Versa Networks. With Fortinet, Lumen SASE Solutions are integrated with Black Lotus Labs-based Rapid Threat Defense to provide automated visibility into identified internet threat detection and remediation.

Limitations

Driving the prominence of Black Lotus Labs Threat Intelligence

The provider's threat research and intelligence team, Black Lotus Labs, has a simple mission to: "leverage our network visibility to help protect our customers and keep the internet clean." This threat intelligence arm leverages high-fidelity information from the telco's global network backbone traffic. This capability is available to clients through security solutions, including the Rapid Threat Defense feature embedded in DDoS mitigation, its Fiber+ network services bundles, network and premises firewalls, and Lumen's Fortinet-based SASE solutions.

In addition, in May 2024, Lumen announced Lumen Defender, a patented solution powered by Black Lotus Labs that identifies and automatically blocks internet-based threats before they breach the customer's internal network.

Lumen must leverage this capability globally to drive awareness and consideration as the provider grows its security capabilities globally. Omdia observes that security intelligence is a valued capability among CISOs and security practitioners, but it is not a highly profitable or commodifiable service. Instead, it generates thought leadership and lends credibility to core security services.

NTT Data (Omdia recommendation: Challenger)

NTT Data should appear on your shortlist if your organization wants an ambitious provider focused on integrated, threat-centric security services

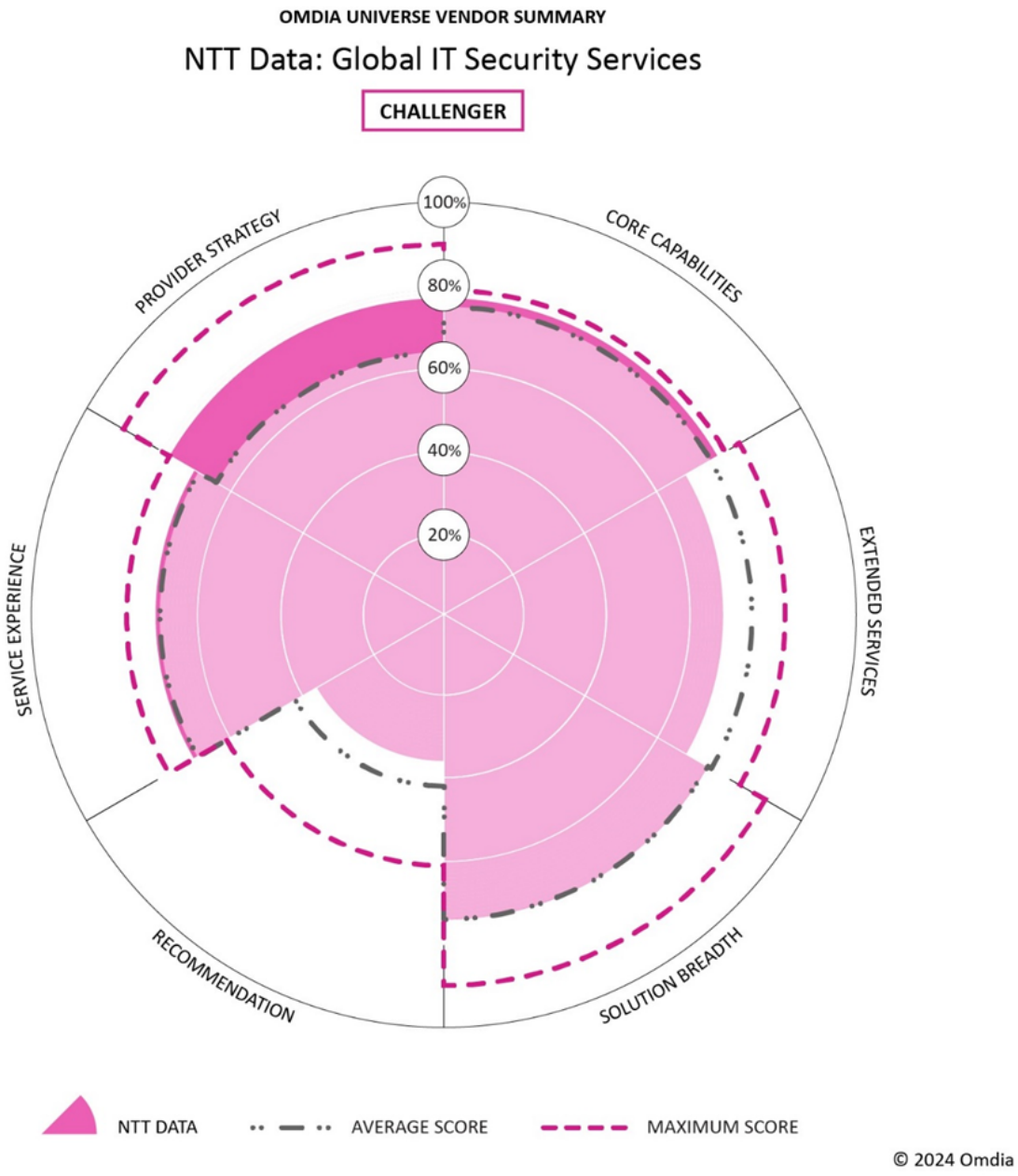
Overview

NTT Data, Inc. is the result of NTT entities merged in October 2022, focused on growth outside Japan. This operating company is part of a three-company structure within NTT Data Group corporate, alongside NTT Data Japan.

The merger of NTT organizations combines complimentary group operating capabilities, $18bn revenue, and more than 150,000 employees into a cohesive structure and unified strategy with a presence in more than 50 countries. Historically, the NTT Group has offerings across consulting, application services, data intelligence, cloud, connectivity, and security. Notable R&D includes the IOWN (Innovative Optical and Wireless Network) global initiative, and the proprietary Japanese large language model (LLM) "Tzuzumi."

NTT Data received an overall customer and service experience score of +31, ranking ninth among established providers. Customers rank NTT Data cybersecurity consulting, integration, and advisory services higher, awarding these capabilities 7.57 out of 10 for service experience.

Figure 16: Omdia Universe ratings—NTT Data



Source: Omdia

Strengths

Long-term focus with a commitment to security and scale

Cybersecurity is an ongoing process. Organizations need a partner to work with them over time to help improve their resiliency in the future. NTT Data has a culturally inspired, long-term perspective across investments and strategy settings, with clear plans and strong capabilities in IT security services globally, including ambitions to drive a large global talent pool of cybersecurity professionals by FY27 through its Talent Development Program. The provider is investing in significant operating model improvements outside Japan, improving security service experiences for current and future clients.

In terms of scale, the provider has extensive systems integration and outsourcing capabilities across many industries, brought together in its new operating structure and strategy. The provider offers eighteen core services in security across consulting and advisory, technology integration, MDR, and crisis response. NTT Data delivers over 2,000 security professionals who provide services from six SOCs and cybersecurity personnel in 80 locations globally.

Limitations

Improving customer recommendation as the new NTT Data

The new group has a solid strategy for global growth in IT security. Customers' perceptions of the provider are shifting, but their impressions of NTT in security services are tracking behind the firm's aspirations. Customers were most likely to recommend NTT's emerging security services and value as a partner for cybersecurity technology—not surprising given that the provider is one of Cisco's most significant partners globally and the biggest in Asia & Oceania.

The provider must continue to develop and demonstrate a global IT security services portfolio outside Japan. Further, as the momentum for the initial announcement wears off, NTT Data can bolster chief experience officer (CxO) consideration by communicating integrated, cross-group, cross-services cybersecurity capabilities, and customer wins.

Orange Cyberdefense (Omdia recommendation: Leader)

Orange Cyberdefense should appear on your shortlist if your organization is seeking a dedicated security firm with a strong European heritage and global footprint

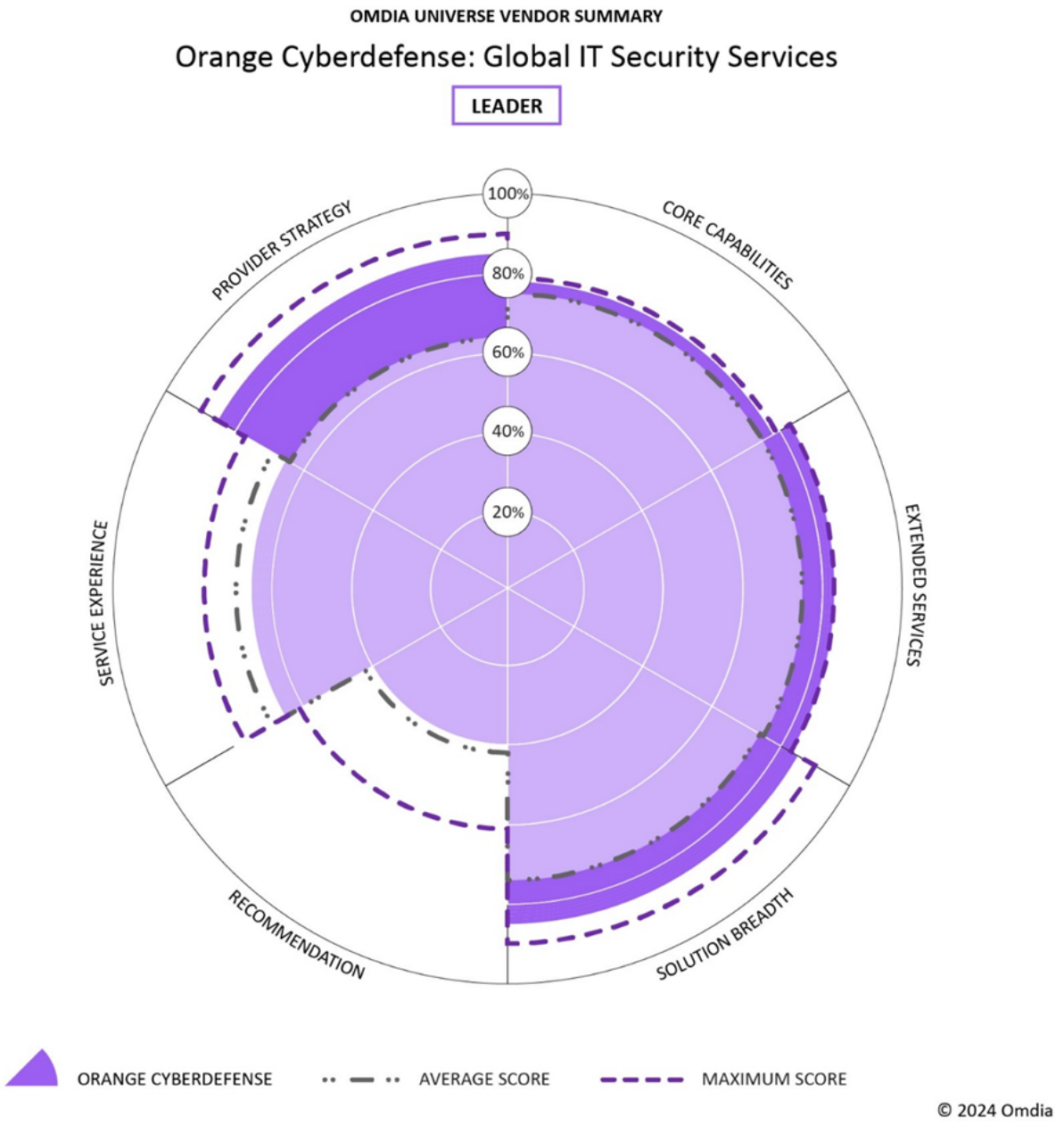
Overview

Orange Cyberdefense is a leader in global IT security and one of the largest dedicated cybersecurity companies globally. The European cybersecurity division of Orange Group reported the fastest organic growth in revenue of any provider for cybersecurity services in this survey. The group scale was bolstered by the 2017 acquisition of two companies—SecureData and SecureLink—and on a smaller scale, the acquisitions of Telsys and SCRT in 2022.

Orange Cyberdefense has one of the most comprehensive offerings in the market and a strong reputation for intelligence-led managed security services and cyberthreat intelligence. The provider has also demonstrated considerable commitment, strategic vision, and solutions capability across various end-to-end security service categories including cloud, endpoint, IAM, OT, SASE, infrastructure, and security intelligence.

The provider achieved a solid customer and service experience, achieving an overall score of +40 in this year's report that ranked Orange second among established providers. The provider also received the third-highest customer recommendation score for industry cyber solutions and high scores in cybersecurity consulting, integration, advisory services, and technology/software across complex environments.

Figure 17: Omdia Universe ratings—Orange Cyberdefense



Source: Omdia

Strengths

Global capabilities forged in challenging European markets backed by deep threat intelligence

Orange Cyberdefense has a strong reputation as a cybersecurity services provider in Europe, expanding into other regions. The provider has achieved over €1.1bn ($1.4bn) in security-specific revenue in 2023, growing at over 11% annually across managed services and consulting. The provider supports nearly 9,000 customers globally from 18 SOCs and 14 dedicated CyberSOCs across North America, Europe, the UK, and Asia including China.

Europe has some of the strictest regulations globally in security and data protection. In this highly regulated market, Orange Cyberdefense has built end-to-end security offerings that map tightly with the NIST Cyber Security Framework (CSF) across all significant domains including cloud, workspace, data, OT, network, SecOps, and TDIR.

Orange Cyberdefense has invested in its intelligence-led security approach and ability to provide early warnings to customers based on proprietary threat intelligence from 500+ sources. The provider has a multidisciplinary team of experts across technologies and vertical industries who can offer a comprehensive, 360-degree view of security. Their agents leverage a proprietary “core fusion” platform and operating methodologies, integrating data from different centers of excellence and security technologies to deliver a single-pane-of-glass view.

In the past eighteen months, Orange Cyberdefense has contributed to thought leadership and research in the security market, notably its Security Navigator report and other deep-dive briefings that range across topics including OT/IIoT Security, Cyber Extortion, and Nation State Threat actors.

Limitations

Expanding global reach and addressing security for digital transformation

Orange Cyberdefense has a comprehensive global portfolio, but the provider’s revenue and origins are still most substantial in Europe. Future growth depends on its expansion into other regions, especially North America and Asia & Oceania, leveraging expertise forged in demanding European markets. It will be essential to ensure consistency of experience across regions as the provider tailors services for new countries and sector-specific needs, as it has done for the public sector in Sweden.

As digital adoption of enterprise applications continues to accelerate, the provider must continue to build out security offerings that address issues such as privacy, sovereignty, and jurisdictional concerns of enterprise data in GenAI (notably LLMs), enterprise databases, and other commercially sensitive applications. Omdia notes that other global systems integrators and IT outsourcing firms have their eye on Asia & Oceania and European markets as well, and are leveraging their credibility established from North America and Asia.

Telefónica Tech (Omdia recommendation: Challenger)

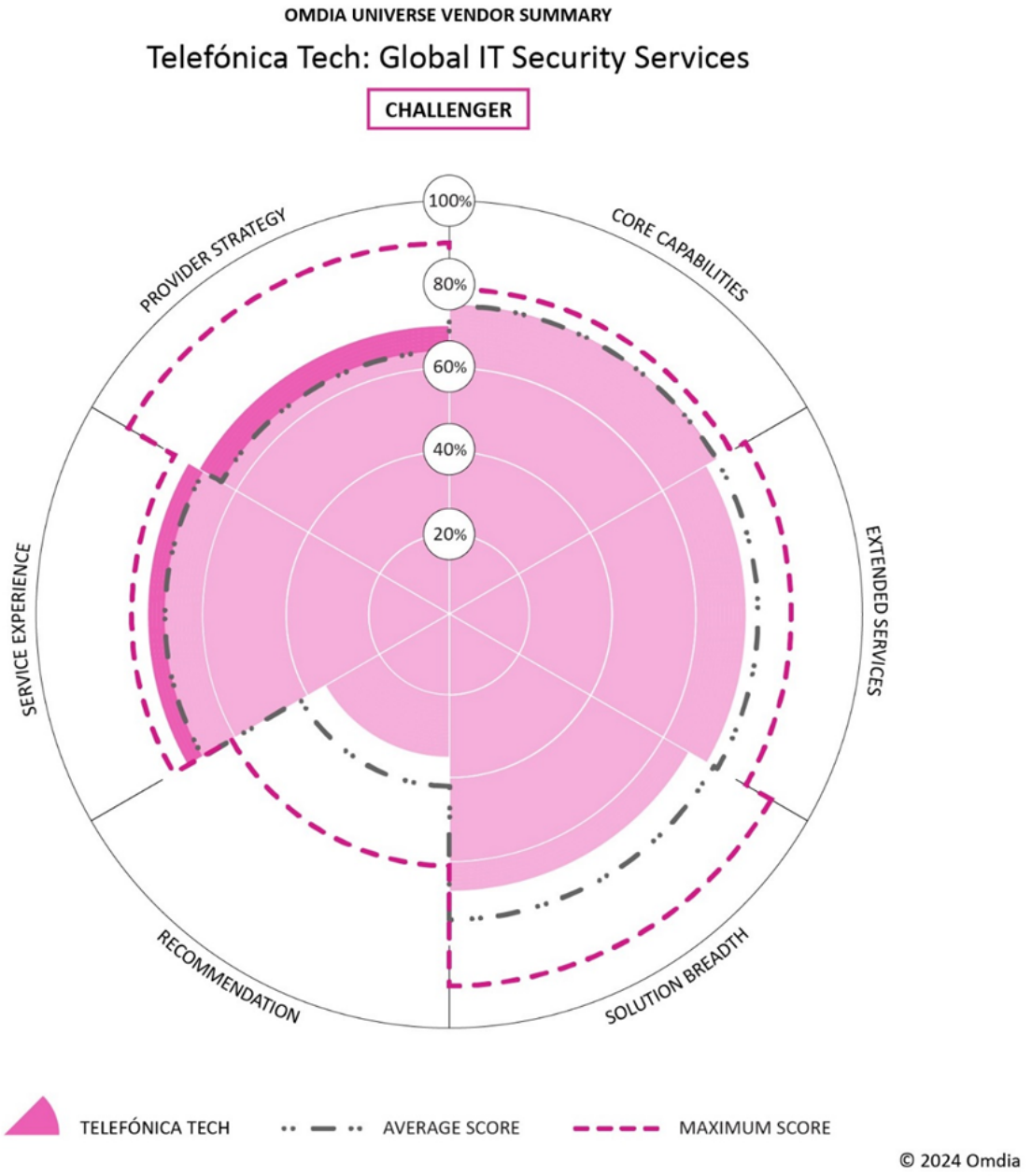
Telefónica Tech should appear on your shortlist if you favor an innovative provider with solid service capabilities across Europe and the Americas

Overview

Telefónica Tech is the B2B global digital unit of the Spanish Telco, Telefónica Global. While the division was formed in late 2019, Telefónica has provided specialized security services that reach beyond network security for well over a decade. Telefónica Tech concentrates on managed and professional services in cybersecurity, multicloud, IoT, and cognitive/AI.

Telefónica Tech achieved an overall customer and service experience score of +28 in this year's report, ranking tenth amongst established providers. Customers are most complementary of the telco’s technology arm for providing cybersecurity solutions.

Figure 18: Omdia Universe ratings—Telefónica Tech



Source: Omdia

Strengths

Broad consulting and services capabilities across Europe and the Americas with consistent innovation and a strong OT security practice

Telefónica Tech is the leading provider in this survey across the Americas. The provider delivers services from a team of more than 2,300 security practitioners globally. MSS is delivered through a primary "Digital Operations Center" in Madrid, linked with 11 "iSOCs" globally, spread across the US, Mexico, Colombia, Peru, Chile, Brazil, Argentina, Ecuador, Spain, and the UK.

Under its “NextDefense” banner, the provider has a broad portfolio of more than 50 cybersecurity services spanning MDR and XDR platforms (NextDefense), TDIR, vulnerability, network, OT, cloud, and IAM security. Telefónica Tech also offers Telefónica’s FlexSuite cloud and security connectivity services, including SASE and cybersecurity consulting expertise.

IT and OT security, including IIoT, is a growing challenge as Industry 4.0 gathers pace and digital services connect physical platforms in critical sectors such as manufacturing and utilities. Telefónica Tech has a clear strategy and compelling security offerings in this market. The provider is creating the first version of an OT-specific SOC that covers customers' cybersecurity needs across OT, IoT, and 5G, leveraging digital expertise in managed XDR, vulnerability, and risk marketing with threat intelligence.

Limitations

Expanding presence into North America and Asia & Oceania, focusing on customer experience

Telefónica Tech has a limited presence outside Europe and the Americas. As a leading presence in Latin America and a considerable scale in Europe, the provider should consider expanding its global focus to reach MNCs in other geographies, especially Asia & Oceania. Language, time zone, and desired customer proximity mean Telefónica Tech needs to double down on MSS capabilities in these target regions.

The Omdia survey of Telefónica Tech customers revealed challenging net recommendation and service experience scores for MSS and Industry cybersecurity solutions. As the provider continues to broaden its offering set, it will be critical for Telefónica Tech to keep positive customer journeys, a single pane of glass, and consistent quality of experience front of mind.

Verizon (Omdia recommendation: Challenger)

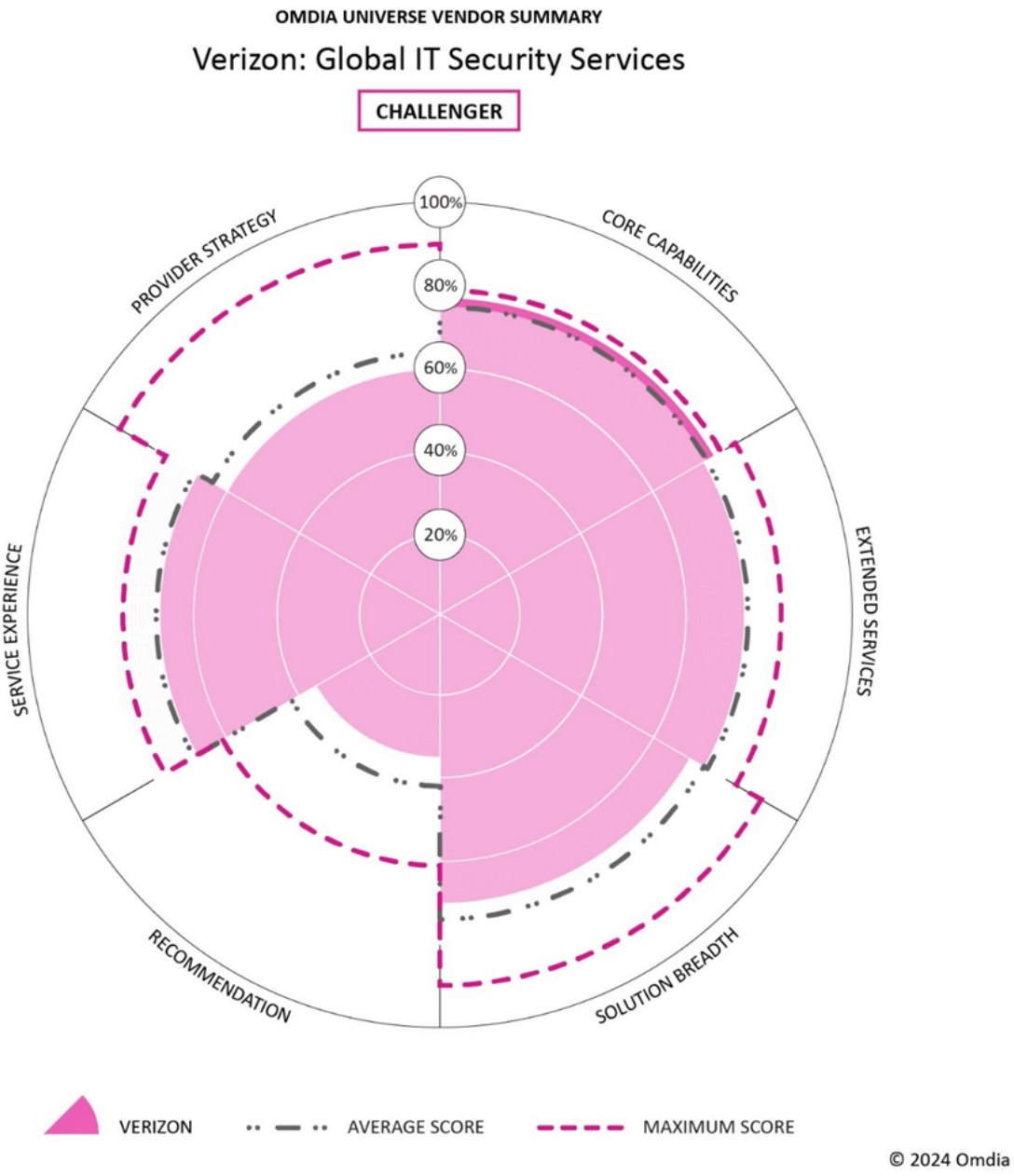
Verizon should appear on the shortlist of enterprises that value a global telco with deep network security capabilities and leading threat research

Overview

Verizon Cyber Security Consulting is part of the Verizon Business Group. More than half of Verizon's B2B revenue is from the global enterprise segment, underscoring the provider’s solid presence in the global enterprise market for ICT services. In August 2023, the provider announced a strategic partnership with HCL Technologies that, among other joint efforts, can deliver managed network services to Verizon's enterprise customers.

Verizon achieved Challenger status in this report, ranking sixth in both overall customer recommendation score (3.2) and service experience (6.82 out of 10) across end-to-end IT security services.

Figure 19: Omdia Universe ratings—Verizon Business



Source: Omdia

Strengths

Robust and scalable, network-based managed security services with leading security research

Verizon has longstanding global experience in providing end-to-end IT security services. Recent strategy briefings reveal that the telco is playing to its strengths and building excellence in security around its core business of national networks, connectivity, and embedded security services in 5G private networks, NaaS, edge, and mobility.

Verizon offers extensive global MSS and professional security services expertise across the three primary regions in this survey: It has nine SOCs globally, three in North America, two in Europe, and four in Asia &

Oceania. The provider has more than 2,000 security professionals distributed across significant regions: six digital forensics labs, six labs for 5G, a security center of excellence, and customer briefing centers.

The provider also has strong in-market thought leadership. Its longstanding Data Breach Investigations Report (DBIR), now in its 17th year, highlights Verizon's deep understanding of industry-led cybersecurity challenges. Other research includes Verizon's "Mobile Security Index Report," "Payment Security Report," and "Verizon Threat Research Tracking Center (VTRAC)" monthly intelligence briefings. This year, the VTRAC team turns 21, a very long-established competence in IT and cybersecurity timelines.

Limitations

Communicating an IT security services vision

Verizon has uniquely deep clusters of security capability embedded in significant regions, including the US, Southeast Asia/Oceania, and EMEA. After expanding its service capabilities over many years, Verizon lately seems to be focusing new security emphasis on the network core and mid-market.

Verizon competes with systems integrators and IT outsourcing providers in managing networks and security, so the HCL Technologies partnership in large enterprises is vital. The partnership has the potential to deepen the security delivery capability of both longstanding and emerging network as a service (NaaS) security solutions to MNCs across both customer bases. Core capability areas include security across SASE, SD-WAN, 5G, IoT, APIs, and edge for Verizon's largest customers.

Omdia recommends that the provider reaffirm and clarify its security ambitions in core markets across enterprises and government with HCL Technologies. The provider should give consideration to its legacy capabilities in markets and regions and can leverage its prominent cyber research, including that from VTRAC.

Other providers

The global IT security services market is a very active space. This Omdia Universe evaluates the most prominent providers against the inclusion criteria. However, there are many providers to choose from. Listed below are additional notable firms that enterprises may evaluate for suitability.

Table 2: Other notable IT Security Services providers

Service provider category	Key providers	Value proposition and competitive differentiation
Systems integrators (SI) and IT services/outsourcing (ITO) providers	Accenture, Atos (Eviden), Cognizant, CGI, DXC, Fujitsu, HCL, Hitachi, IBM, Kyndryl, Infosys, HCL Technologies, Persistent Systems, Tech Mahindra, and Wipro	• These providers have vast scale and depth of expertise in various technologies, tools, and practices, including cybersecurity. Managed security is a large but low–medium revenue growth area. • However, as a service category, it is crucial as many MNCs and government agencies require third-party expertise to meet compliance needs and secure complex digital transformation programs.
Telecommunications providers/communication service providers (CSPs)	AT&T Cybersecurity, America Movile, BT, China Telecom, Chunghwa Telecom, Lumen, Colt, NTT Data, Orange Cyberdefense, Starhub, Tata Communications, Telecom Italia, Telefónica, Telecom Argentina, Telkom (SA), T-Systems, Telstra Purple (Asia & Oceania), Singtel, Verizon, and Vodafone	• CSPs have massive scale and vast network expertise, affording unique security telemetry. Several have established or spun off partially separated business units to focus exclusively on cyber. • Security is increasingly important as virtualization becomes more pervasive across networks, infrastructure, and applications, and MNCs require telco scale and presence in MSS.
Management consulting	AT Kearney, Booz, BCG, Capgemini, Deloitte, EY, KPMG, McKinsey, and PWC	• Management consulting, technology, and professional service providers have diversified into security, across from tax and audit, risk, strategy, and organizational change. • These firms invest in cybersecurity consulting practices that leverage strong

		brand trust and unique access to the C-suite (from other consulting practice areas), and some offer MSS.
Security appliance, SaaS, and independent software vendors (ISVs)	Broadcom, Checkpoint, Cisco, Fortinet, F5, Microsoft, OpenText, Palo Alto Networks, Proofpoint, Secureworks, Symantec, and Zscaler	• These providers leverage platform, process, and architectural intellectual property in security to offer clients direct sale design, implementation, technical support, training, and basic management services (platform-specific). • They rely primarily on other providers in this list to resell and manage cyber in more complex environments and at scale.
Specialists and regional players (including MDR)	Arctic Wolf (US), Cisco, Crowdstrike, Clearswift/HelpSystems (UK), Critical Start CyberCX (Asia & Oceania), Expel, eSentire, Fortinet, Palo Alto Networks, Red Canary, SentinelOne, Sophos, Trend Micro Secureworks, and Mandiant (Google)	• There are dozens of regional and specialist security platform providers offering fundamental MSS, MDR, SOC as a service, and professional security services. In this report, some predominantly sell through more significant partners, although many sell some basic services directly where customers demand it. • This category of security providers is proliferating, and we expect substitution from fully managed MSS to MDR over time as platforms become more intelligent and firms consolidate tools.

Source: Omdia

Appendix

Methodology

Omdia Universe

Omdia's rigorous methodology for the Universe product includes the following:

- The invitation to participate was set against high-standard inclusion criteria across presence, scale, and capability.
- Omdia evaluates providers based on an in-depth market understanding, using proprietary market forecasting data, custom surveys, and enterprise insights survey data.
- Omdia evaluates providers across a matrix of capabilities, attributes, and features that it considers essential for the market now and in the next 12–18 months.
- Participating providers are interviewed and provide in-depth briefings on the current capabilities, solutions, and strategy for growth.
- Analysts supplement these briefings with other information from industry events, user conferences, and internal collaboration forums.
- The Universe is peer-reviewed by other Omdia analysts before being proofread by a team of dedicated editors.

Inclusion criteria

Benchmarking in the Omdia Universe (chart) requires meeting the following criteria:

- **Presence:** The provider can deliver IT security service (cybersecurity) capabilities across two or more significant regions, including North America, Europe, Asia & Oceania, the Middle East, and Africa.
- **Scale:** Last year, the provider realized significant global revenue from cybersecurity and IT security services of >$200m.
- **Capability:** The provider can deliver a comprehensive range of cybersecurity services across two or more categories: managed security services, security consulting, professional services, industry cybersecurity solutions, and third-party solutions/channel programs value added resellers (VAR).
- **Focus:** The provider can demonstrate a strong focus on cybersecurity as a strategic corporate growth priority.

Note: Some providers may be included in the report as representative firms (not benchmarked) where only one of these criteria is met and remains at the analysts' discretion.

Scoring

- Customer and Service Experience is the weighted average of the “likelihood to recommend,” “service provider experience,” and analyst determination, based on scores in IT security from an Omdia-commissioned primary research survey conducted in 2024 of more than 220 senior IT decision-makers at large enterprises and governments. Customers must have purchased specific security services from the provider in the past twelve months to provide ratings.
- Solutions Capability and Strategy is the analyst-determined security services capability across all domains, including managed services, cybersecurity consulting, emerging & innovative services, industry cybersecurity solutions, and VAR.
- Market Presence is based on analyst assessments of provider-reported revenue in security-specific services, excluding OEM.

Assumptions

This report focuses on large MNCs, governments, and large enterprises:

- This report focuses on the holistic security buyer needs of Fortune 500 MNCs and governments. Future editions may explore the mid-market (circa 1,000+ employees).
- Global capabilities focus on the largest addressable markets, including North America, Europe, and Asia & Oceania. Future editions may expand deeper into other regions, including the Middle East, Africa, Latin America, and the Caribbean.

Scores are calibrated within each revision to reflect market shifts:

- In all cases, the Omdia assessment best uses provider-supplied RFI content, private briefings, publicly available material, analyst assessments, and analyst community briefings to assess capabilities, commitment, and strategy across complex, end-to-end cybersecurity services.
- All ratings, vendor analyses, and the Omdia Universe report have undergone a rigorous, internal peer review process among Omdia’s subject matter experts.
- Customer experience scores reflect a statistically significant number of senior decision-makers' ratings from customers of participating service providers across specific security services.

Participation:

- Not all providers actively participated or were able to respond to both RFI and briefing components, and each provider responded with different degrees of depth and breadth. Of note: Accenture, DXC, IBM, NTT, and Verizon declined to actively participate in this edition. BT provided limited input.
- Participating providers supplied confidential sources under NDA that were used in the benchmarking scores.
- Many providers could not disclose regional revenue splits due to company policy. Revenue numbers used for market presence are Omdia estimates.
- Providers had the opportunity to fact-check their respective sections before publication.

Further reading

Global Managed Security Services Forecast Updates and Trends: 2024–28 (November 2023)

Omdia Universe: Global IT Security Services Provider, 2022–23 (October 2022)

Omdia Universe: Selecting a Global IT Security Services Provider, 2021 (March 2021)

Author

Adam Etherington, Senior Principal Analyst

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com