Publication date: 12 Jun 2024

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

This edition of the report has been abbreviated for redistribution.

Omdia Universe: Global IT Security Services Providers, 2024



OMDIA

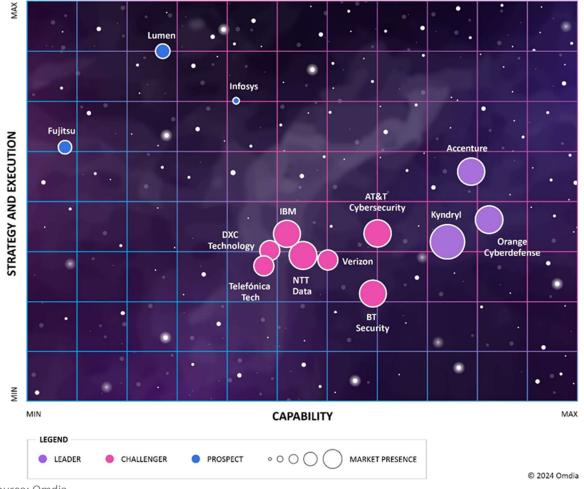
UNIVERSE

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



OMDIA UNIVERSE: Global IT Security Services

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.

- ΩΝΩΙΛ
 - 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

- Accenture, Orange Cyberdefense, and Kyndryl are Leaders, demonstrating the most substantial global capabilities in IT security services across solutions capability & strategy dimensions. Leaders also achieved meritorious customer & service experience results at scale.
- AT&T Cybersecurity, BT Security, DXC, IBM, NTT Data, Verizon, and Telefónica Tech are *Challengers*. These providers offer extensive end-to-end capabilities and achieved robust customer & service experience scores across a large customer base.
- Fujitsu, Lumen, and Infosys are Prospects. These providers are new additions to this report edition and performed well as leaders in select markets and pockets of emerging cybersecurity services. All prospects achieved outstanding customer recommendation scores.

© 2024 Omdia

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.

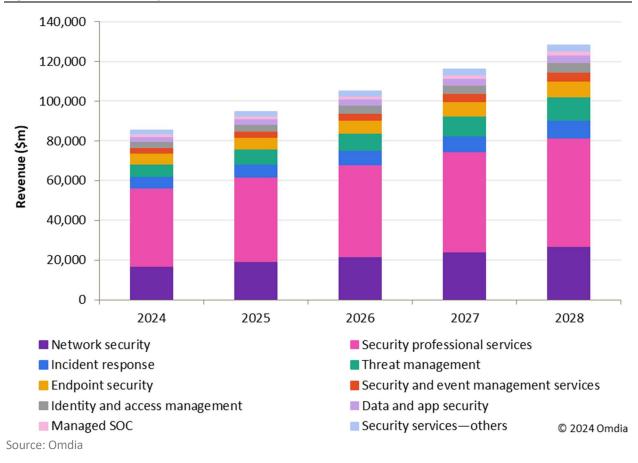


Figure 3: Global IT Security Services Forecast, 2024–28 (\$m)

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

Market <i>Leaders</i>	 Leaders demonstrate capability and commitment to delivering the most comprehensive, well-integrated, and end-to-end cybersecurity solutions globally. These providers offer capabilities across most service categories, geographies, and industries. Leaders also have above-average customer experience and service scores from Omdia's independent survey(s).
Market Challengers	 Challengers offer highly integrated security service capabilities in two or more significant geographies. These providers are often more specialized, focusing on fewer security solution capabilities and regions than <i>Leaders</i>. Challengers have customer experience and service scores comparable with the market mean in Omdia's independent survey(s).
Market Prospects	 Prospects, compared to other providers assessed, focus on a limited number of service capabilities and regions, have smaller scale & revenue, or are new to the Universe assessment. Nonetheless, Prospects demonstrate considerable commitment and expertise to global IT security. In Omdia's independent survey(s), Prospects' customer experience scores were typically lower than Leaders' or Challengers'.

© 2024 Omdia

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:

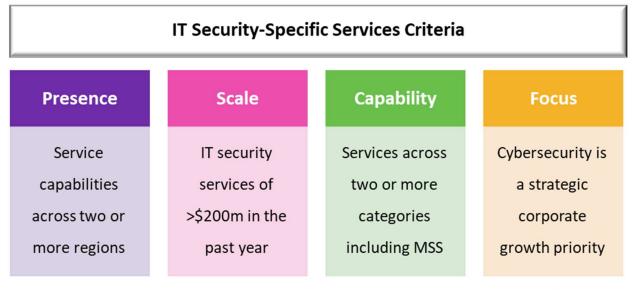
• Established Providers: This survey benchmarks IT security service providers, including Accenture, AT&T Cybersecurity, BT Security, DXC Technology, Orange Cyberdefense, IBM, Kyndryl, NTT Data, Telefónica Tech, and Verizon Business.

- 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



© 2024 Omdia

Source: Omdia

Universe ratings and scoring

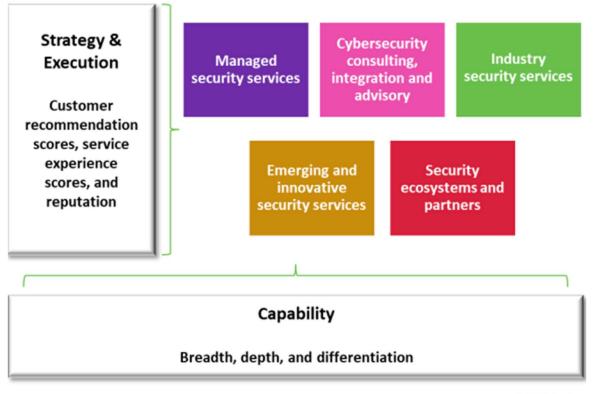
As **Figure 1** illustrates, the overall Omdia Universe ratings reflect scores across the overall Strategy and Execution (Y-axis) and Capability (X-axis).

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



© 2024 Omdia 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

Kyndryl (Omdia recommendation: Leader)

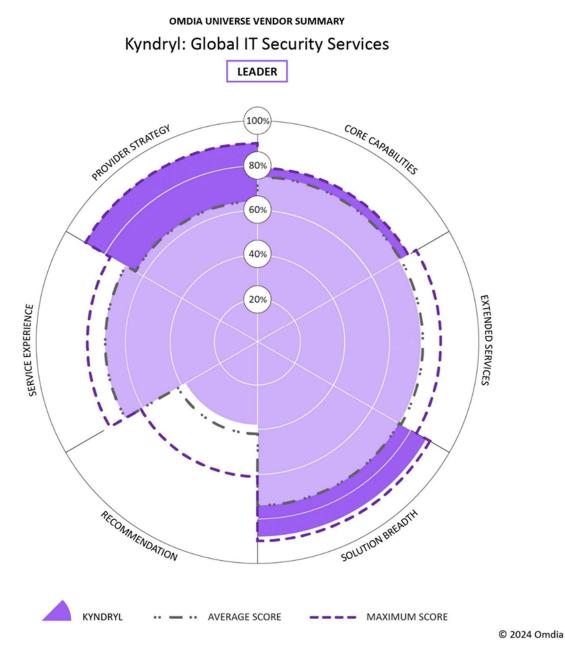
Kyndryl should appear on your shortlist if your organization has complex infrastructure focused on cyber resilience and recovery Overview

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.

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 securityspecific 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

<u>Global Managed Security Services Forecast Updates and Trends: 2024–28</u> (November 2023) <u>Omdia Universe: Global IT Security Services Provider, 2022–23</u> (October 2022) <u>Omdia Universe: Selecting a Global IT Security Services Provider, 2021</u> (March 2021)

Author

Adam Etherington, Senior Principal Analyst

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via <u>citations@omdia.com</u>.

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 <u>consulting@omdia.com</u>.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

<u>omdia.com</u>

askananalyst@omdia.com