OMDIA UNIVERSE

Publication date
06 October 2022

Author
Adam Etherington
Principal Analyst
Digital Enterprise Services

Global IT Security Services Provider, 2022–23

OMDIA

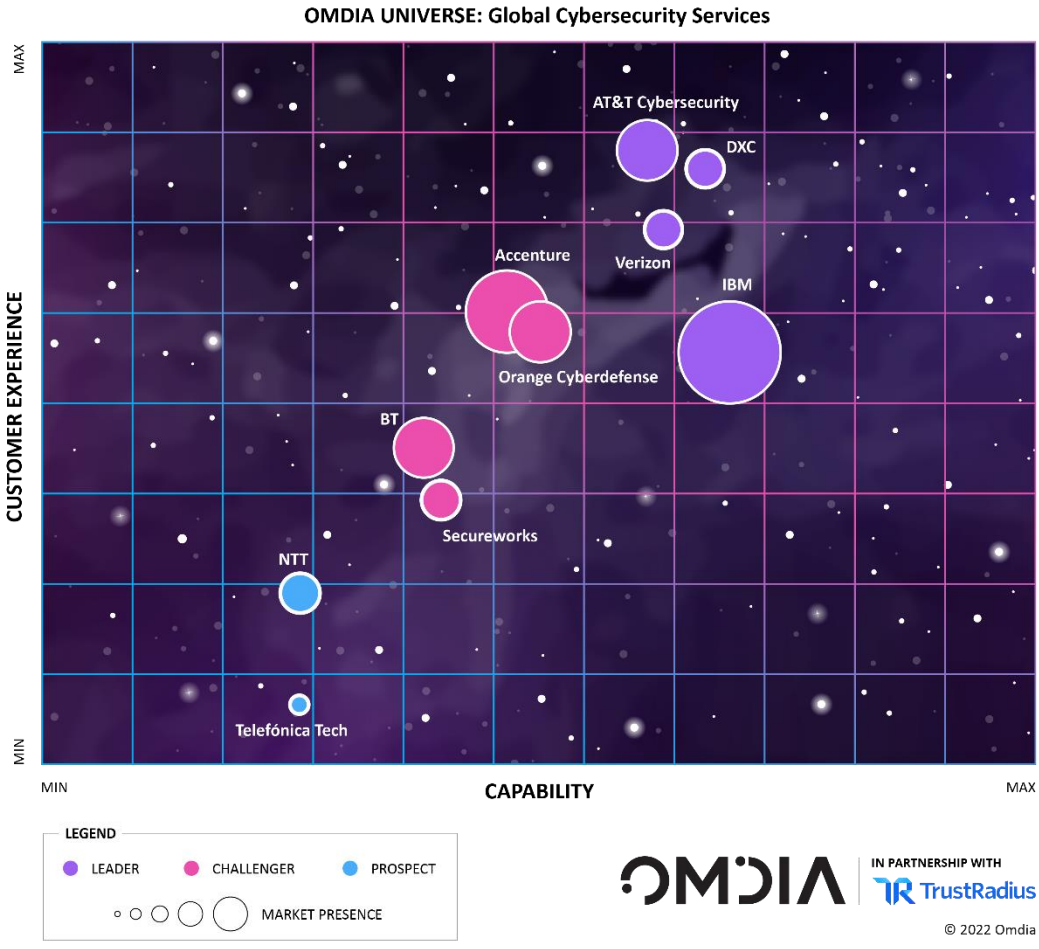
Brought to you by Informa Tech

Summary

Catalyst

This Omdia Universe offers an independent, comprehensive, end-to-end assessment of leading global IT security service providers across two significant dimensions—customer experience and overall solution capability.

Figure 1: The Omdia Universe for Global Cybersecurity Services (IT security)



Source: Omdia

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

The comprehensive benchmarking conducted for this report assessed a broad range of services: consulting; professional services; managed security services (MSS); cybersecurity consulting, integration & advisory; threat detection & intelligence, industry cybersecurity solutions; and cybersecurity technology & software. These services are the foundation of any modern large enterprise and government organization.

We trust that this Universe will assist any CIO, CTO, or chief information security officer (CISO), and any other senior decision-makers responsible for shortlisting providers best suited to their security requirements.

Omdia view

In this 2022 updated edition of the Omdia Universe for Global IT Security Services:

- **IBM, Verizon,** and **DXC** remain market leaders, scoring exceptionally well across customer experience and service capability dimensions.
- **AT&T Cybersecurity** is now a leader. Customers awarded the provider greatly improved recommendation scores. Capability scores rose from industry security capabilities and progressed integration across security and network services with underlying platforms.
- **Secureworks, Orange Cyberdefense, and BT** have extended security capabilities, lifted capability scores, and closed the gap with market leaders since the last report.
- **Accenture** continued to acquire capabilities and offer extensive scale, breadth, and experience in complex IT environments; however, limited innovation and not having a clear strategy sustained their Challenger position.
- **NTT and Telefónica Tech** are new additions to this year's assessment, and performed well as Prospects with good regional, end-to-end cybersecurity services capabilities.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Understanding the IT Security Services Universe

How to use this report

Cybersecurity is increasingly complex and mission-critical. Not all firms are equally prepared. Digital dominance demands they must be.

While every firm is ultimately responsible for its cyberdefense, risk, and compliance, the degree to which each organization engages third parties to assist differs considerably. Consequently, executives will naturally consider various security services to overcome broad-ranging challenges.

This benchmarking report and analysis will help decision-makers shortlist an IT security services partner.

The evaluative criteria in this report cover five major IT security service areas: MSS; cybersecurity consulting, integration, & advisory: threat detection & intelligence: industry cybersecurity solutions; and cybersecurity technology & software (value-added resellers (VAR)).

This report can guide, inform, and expedite a selection process to match provider capability to multi-national companies (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.

Omdia Universe scope and methodology

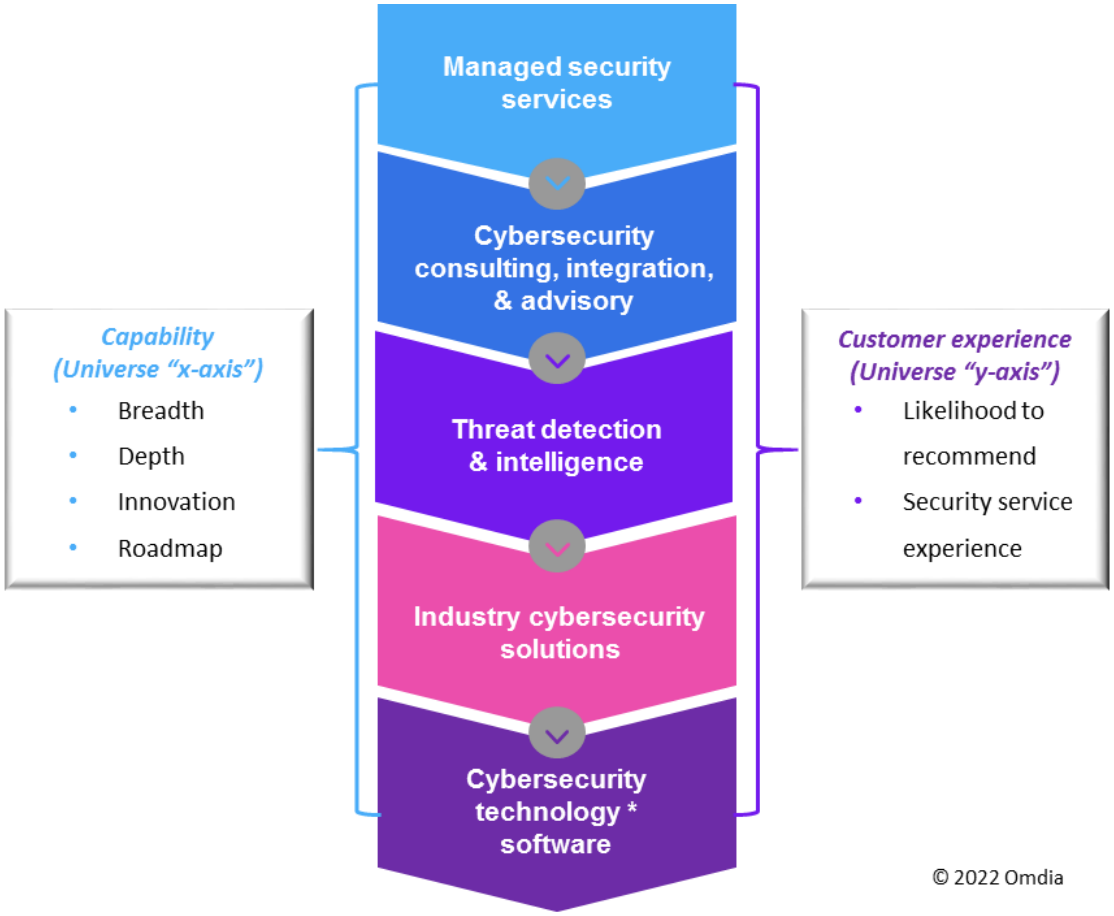
This report benchmarks global service providers into Leaders, Challengers, or Prospects categories in global IT security services.

Selection Criteria: Omdia invited providers to participate to demonstrate that they met the inclusion criteria. Benchmarking in this report draws on provider responses, a direct survey of over 130 senior decision-makers with experience with these service providers, Omdia analyst assessments from publicly available information, and service provider analyst briefings.

Universe ratings: Scores reflect a weighted average score across two dimensions, as illustrated in **Figure 2**.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 2: Omdia Universe scoring—IT security services



Source: Omdia

Capability: A weighted average capability score reflecting each provider's global strategy, innovation, differentiation, breadth, and depth of services across all security services (horizontal axis in the Universe chart (**Figure 1**)):

- **Customer Experience:** The weighted average score of "likelihood to recommend" and "service provider experience" from an Omdia-commissioned primary survey of service providers' end customers (vertical axis in the Universe chart).

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Omdia Universe award categories

- **Market Leaders:** Offer the most comprehensive, well-integrated, end-to-end cybersecurity solutions available globally. Leaders also have above-average customer experience scores.
- **Challengers:** Offer a high degree of integrated security service capability and positive customer experience. Challengers usually excel in one or more service domains and regions, with average customer experience scores.
- **Prospects**: Typically, newer entrants and regional providers have niche capabilities not as tightly integrated as other providers. Customer experience scores were lower than average.

Market definition: Global IT security services

Global IT security services encompasses standalone and integrated service capabilities spanning managed services, consulting, industry solutions, and VAR (see **Figure 3**).

Each provider assessed in this report frequently uses different terms for comparable services. Omdia defines five categories in this Omdia Universe for consistency and comparison to capture the most critical, holistic IT security services.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 3: Omdia Universe scoring methodology—Core IT security service categories assessed

Source: Omdia. An expanded Taxonomy is also available later in this report

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Market dynamics

IT security services (cybersecurity)

Modern organizations are increasingly digital, leveraging hybrid IT to align technology with business outcomes. Firms continue to migrate critical applications to the cloud, workers remain in remote/hybrid working models, and governance/compliance measures will tighten.

Combine this with global uncertainty from geo-political tensions, the Russia–Ukraine war, cyber-warfare, economic volatility post-pandemic, and tightening monetary policies, and boardrooms worldwide are hardening their stance on risk and demanding more from security leaders.

As a result, cybersecurity is increasingly a critical requirement for digital resilience and competitiveness.

Unfortunately, Omdia's research confirms that large organizations across all major sectors have experienced an increase in the volume and severity of cyberattacks. A third of all firms surveyed saw a significant increase (more than 25%) in security incidents across their IT estate last year. Attacks on the cloud, enterprise data systems, and supply chain (third-parties) jumped materially.

The attack surface continues to grow as digital value chains link suppliers and end customers into core systems. Navigating the shared responsibility model in hybrid cloud architecture is often a concern. Simultaneously, skills shortages and high cybersecurity staff costs continue to be a considerable challenge burdening already-strained SecOps teams.

In this dynamic context, the IT security providers in this report assemble unique combinations or geographically dispersed cyber capabilities to ameliorate cyber challenges.

Most organizations (54%) now engage a third-party security service provider under an ongoing contractual relationship or ad-hoc engagement. Flexibility, breadth and depth of security expertise, innovation, certifications are the key drivers. Cost is essential, but a lower order priority in the face of rising risk and material impacts from a breach.

Core themes in this year’s report

Ongoing cyber disruption, advanced threats

Since 2021, the market for IT security services accelerated at a faster pace than many thought likely. Notable cyber incidents punctuated the period, and the likelihood of a “Severity 1” security incident or breach is rising.

Recent examples of critical infrastructure attacks, major ransomware incidents, notifiable data breaches, embarrassing cloud misconfigurations, and intricate supply chain attacks underscore the threat.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

According to the World Economic Forum, targeted and sophisticated cyberattacks are multiplying and increasing faster than most organizations and governments can prevent, detect, and respond to those attacks. Omdia has observed a spate of financially and politically motivated attacks on organizations and governments.

The known vulnerabilities are long. At its last count, the Cybersecurity and Infrastructure Security Agency (CISA) listed over 683. The US National Institute for Standards and Technology (NIST) has over 16,000 Common Vulnerabilities and Exposures (CVE) logged. The number of exposures is staggering.

Organized adversaries, purposeful attacks

Organized criminal groups and nation-states are frequently behind many cyberattacks. Recent examples include the North Korean State-Sponsored APT targeting blockchain companies. Russia's invasion of Ukraine had reports of cyberattacks on the Ukrainian government and critical national infrastructure. CISA and its Joint Cyber Defense Collaborative (JCDC) launched the "Shields Up" campaign and knowledge base in early 2022. The technical resources address Russian threat actors, ransomware, destructive malware, distributed denial of service (DDoS) attacks, and protective measures in anticipation of more significant risks and attacks to the broader region, not just Ukraine.

Across different threat actors, reports from victims and global security providers are unanimous; most attackers are well-equipped, leveraging technology in nefarious ways to exploit common vulnerabilities and zero-day exploits. Pertinent examples include botnet DDoS attacks, intricate supply chain infiltration, ransomware-as-a-service kits, and double extortion tactics.

Perhaps most disturbing are the malevolent cyber innovations happening. One example is the alternative monetization methods with Monero to help obfuscate financial breadcrumbs left behind on other blockchain ledgers. Another is ransomware-as-a-service to equip malicious intent with better capability. Or consider the May 2022 cloud threat, forcing the CISA Emergency Directive 22-03 to mitigate VMware vulnerabilities. Attackers reverse-engineered an update to drive deeper exploitation of unpatched services.

CISOs under pressure

Spare a thought for the ardent technology executives. They face ongoing calls to arms from business executives within their organizations to innovate without greater risk exposure. Yet most boardrooms have a limited understanding of cybersecurity risks and are wary of potential personal liabilities from a ransomware breach or failed regulatory audit.

Spending on security is forecast to rise. In a recent Omdia global survey, cybersecurity was the top spending priority among executives, ahead of digital customer engagement tools and intelligent automation.

Many, if not most, CISOs will nonetheless argue that budgets aren't increasing fast enough to address dramatic threat increases and dependencies by the business on digital technologies.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Skills shortages bite

Skills shortages is cited by 32% of global decision-makers as a significant challenge in cybersecurity. As seasoned executives know, hiring a professional cybersecurity individual who is business savvy with gleaming security credentials is a utopia—and rarely is economically viable. The digital economy—marked by more remote workers, integrated supply chains, hybrid and multicloud, Agile practices, and microservices architecture—made for a lethal combination of complexity, and one dependent on talent to solve.

Emerging solutions evolve

The technology market has responded with many "solutions." Take your pick: SASE, zero trust, XDR, MDR, AI/ML infused platforms, proprietary threat intelligence, next-gen SIEM, and many others. Undoubtedly there is value in choosing the right solution, leveraged by skilled professionals, empowered by mature processes and governance, and supported by tech-savvy senior executives and boardrooms. However, it is an ongoing challenge to know what you have and need, and then harness them to improve organizational security posture. Organizations need fewer tools (or better-integrated ones), not more. Stovepipe and swivel-chair operations are inefficient, burn out staff, and expose gaps in a firm's security posture.

Historical bifurcation of tools, data complexities, and securing hybrid IT will drive increased demand for integrated toolsets across threat detection and response. Accompanying services enablement across implementation, upskilling, change management, and SecOps will drive demand for service providers. They have experience at scale across multiple customers and platforms (many with their own or tightly aligned to third-party vendors). The providers also bring industry-specific expertise in various service models to unify threat detection and response capabilities.

High customer expectations

Not all service providers are equal in expertise, nor are they judged so by customers. A core part of this Universe report is the independently commissioned customer experience survey regarding the likelihood of recommending and rating the quality-of-service experience among benchmarked providers.

The likelihood of existing customers to recommend their security service provider ranged from a net score (low score giving detractors less high score giving promotors) of -4 to +45 this year. The average recommendations score dropped by 8 points year on year (YOY). As a result, providers that maintained or even improved scores this year bucked a trend and are a standout.

The customers Omdia spoke with in developing the assessment knew what their providers were good at, felt well supported, had confidence in their expertise, and judged their organizations were getting incremental value despite the additional costs.

Several executives also mentioned the ability to drive faster and more widespread change into their business by using a third party to arbitrate, advise, and facilitate change management at scale in staff awareness and training and cloud security.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Service provider investments

All providers are investing in or have committed to evolving MSS. Managed threat detection and response—applying machine learning, AI, and automation—expanded automated security orchestration capabilities, and deepened threat intelligence, hybrid cloud security, and growing third-party ecosystem partnerships.

These investments are all focused on supporting the improvement of organizational security postures and play a key role in security controls. But, of course, tech on its own is insufficient, and we need people and process improvements over time to buffer organizational cyber resilience.

Further, providers benchmarked in this report have assembled varying skills, industry experience, market commitment, innovation, breadth, and depth of services across security-specific domains. Capabilities range from managed services, consulting, threat intelligence, industry services, and technology-based solutions for large MNCs/government/public sector, and increasingly, enterprises, non-government organizations (NGOs), not-for-profits (NFPs) and the mid-market (999–5,000 employees)

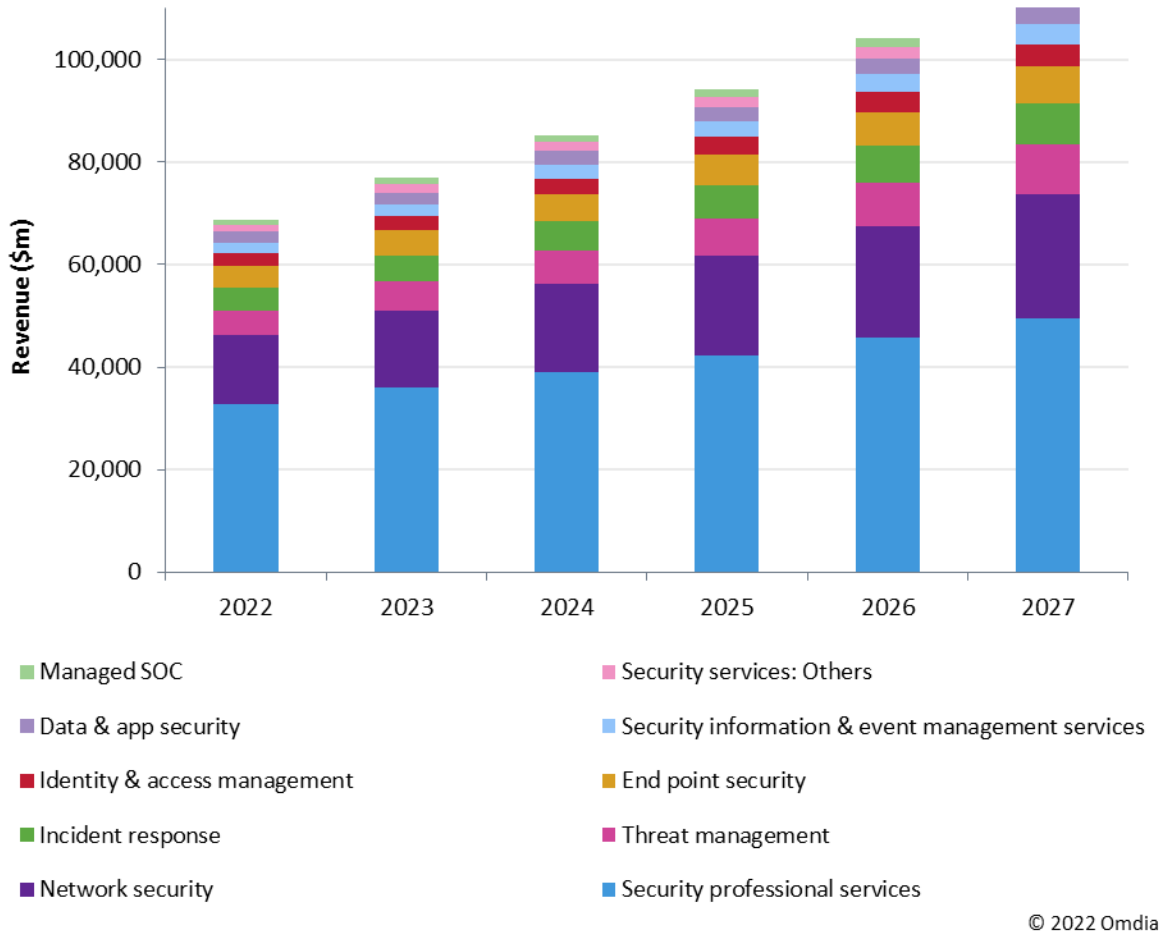
© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Market outlook

Omdia forecasts the global cybersecurity services market will reach $102bn by 2026, a CAGR of 10.8% over the 2022–26 period. IT security has accelerated as a spending priority, and it is among the fastest addressable services growth markets.

Figure 4 shows the global cybersecurity market forecast from the Enterprise Services Total Addressable Market Spotlight Service.

Figure 4: Global IT Security Services Forecast, 2022–27 ($m)



Source: Omdia Digital Enterprise Services Total Addressable Market

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Service provider analysis

Verizon (Omdia recommendation: Leader)

Verizon (VZ) should appear on shortlists for enterprises that value a global telco with broad security capabilities, 5G and cloud security innovation, strong client references, and positive overall peer recommendations in security

Verizon retains a firm market leadership status in this year's report, and has been rated an impressive third in overall peer recommendation scores with +45.

The provider also achieved high customer service satisfaction ratings in threat intelligence & detection, consulting & integration, and MSS.

Verizon offers extensive professional services-led security capabilities, backed by global MSS expertise across all major regions in this survey. It also leverages extensive thought leadership, notably the longstanding DBIR, to highlight a deep understanding of industry-led cybersecurity challenges.

Table 10: Verizon—Key cyber statistics

Security revenue	$600m (estimated)
Security professionals	~2,100+ (estimated)
SOCs	Nine globally: three in North America, two in Europe, and four in Asia and Oceania
Key partners	Palo Alto, Cisco, Zscaler, Crowdstrike, Fortinet, Netskope, Qualys, Juniper, Bitsight, iboss, Tanium, Recorded Future, Anomoli, Delinea, Securonix, Onapsis, Guardtime, Acalvio, CheckPoint, Tenable
Thought leadership	Extensive reports, webinars, advisory services and insights, including: "Data Breach Investigations Report" (DBIR, now in its 15th year), "Mobile Security Index Report," "Payment Security Report" and "Verizon Threat Research Tracking Center (VTRAC) Monthly Intelligence" and alerts.

Source: Omdia

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 14: Omdia Universe ratings—Verizon

Source: Omdia

Service provider summary

Verizon Security Services resides within the Verizon Business Group, and are among the fast-growing services offered to enterprise and public sector customers from the company. Approximately 62% of Verizon's B2B revenue is from the global enterprise segment, highlighting a solid presence in the global MNC IT services market.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

The service provider has a clear, publicly available security services strategy backed by a global commitment to flexible service delivery across consulting and MSS in critical sectors.

Continuing innovation in cyber includes Secure Accredited Gateway Environment (SAGE), Verizon Advanced Secure Access Service Edge (SASE), and multiple consulting offers spanning zero trust, pointed compliance, risk assessments, & incident response services.

Verizon Security Services are provisioned through nine global SOCs, distributed across significant regions, six digital forensics labs, six labs for 5G, a Security Center of Excellence, and customer briefing centers.

Universe assessment

Verizon's strengths include high customer recommendations, broad security services capabilities, security thought leadership, notable security service investments, and strong references

A persistent leader in peer recommendation and service experience

Verizon achieved positive year-on-year advocacy ratings. Customers rated Verizon's security service experience most highly in threat intelligence & detection, ranking it first. In consulting & integration, and MSS, Verizon ranked third for quality of experience.

Excellent breadth of security services

While not the largest service provider by security revenue, Verizon punches above its weight in professional services, managed services, and industry solutions. The provider offers a broad portfolio of security services globally, complemented by an ecosystem of diverse technology partners.

Recognized as a security thought leader

Verizon has achieved standout thought leadership and offers clients deep cybersecurity insight and knowledge as both producers and consumers of cyberthreat intelligence.

Verizon regularly publishes reputable industry reference guides, leveraging intelligence and data-based services from decisions and actions to support customers globally. Reports include the *Verizon Data Breach Investigations Report* (DBIR), now in its fifteenth year, and *Incident Preparedness and Response*, *Mobile Security Index*, and the *Payment Security Report* (PSR).

Cyber innovations

Verizon is well-positioned for growth around the network and digital transformation with compelling roadmaps that address the security and industry challenges of emerging technologies such as blockchain, IoT, quantum computing, and AI/ML.

Recent cyber solution launches include integrated PKI authentication, a ransomware attack simulation service, Log4j assessment, and customer engagement enhancements.

Notable investments include:

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

- **Secure accredited gateway environment (SAGE):** A cloud-based secure internet gateway solution that combines gateway infrastructure protection, customer gateway services, and common service environments (e.g., portal, advanced analytics) into a standardized, scalable solution set. The solution is purpose-built for government compliance and, while currently launched in Australia, highlights industry-level platform and service capability potential.

- **Evolving managed detection and response:** Verizon invests in managed detection and response that delivers continuous (24/7/365) real-time alert monitoring by Verizon Security Operations Center (SOC) analysts with incident validation and management, containment and disruption, and support for custom playbooks. Verizon Threat Research Advisory Center (VTRAC) and third-party providers, including Recorded Future, underpin threat detection related capabilities.

- **Verizon advanced secure access service edge (SASE):** Merges software-defined wide area network (SD-WAN) capabilities with internet threat protection (Secure Web Gateway) and zero-trust network access (Zero Trust). The solution incorporates managed and professional services levels by Verizon NOC and SOC experts.

Firm marquee client reference

Verizon also provided a high-profile Asia-based global MNC client reference. Delivering advanced SOC services for the client's mission-critical systems, they commended Verizon for bringing "amazing" global scale and expertise to bear with local agility over time.

Opportunities and threats to Verizon include other Universe telcos rapidly investing in security and pressure from integrators that offer end-to-end transformation capabilities through deep client relationships.

Stiff competition on multiple fronts

Digital transformation is the next frontier of cybersecurity services. Verizon will increasingly face off against global integrators and managed services providers with deep client relationships in large enterprise and government client segments.

Verizon's competitors leverage extensive industry-specific security expertise, enterprise architecture, in-depth consulting, and integration experiences to identify and address cybersecurity challenges. Verizon's opportunity is to lead security around digital transformation enabled by IoT, 5G, and network transformation.

Increasing scalable platform capabilities

Verizon's key competitors invest heavily in highly scalable advanced platforms that address SIEM, SOAR, XDR, and advanced MDR use cases. Verizon has a robust set of technology alliances that underpin its solutions, and not being tied to one platform is a differentiator among some customers.

Future success opportunities exist in markets where services and platforms are becoming interwoven by automation, requiring continued focus on security solutions that extend across the

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

entire topography from network, cloud, mobile, 5G, MEC, and IoT. Further, Verizon could leverage SOAR and MDR/EDR to accelerate compromise detection and optimize mitigation efforts, consumable via a single user interface.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Omdia Universe methodology, IT security services

Omdia Universe chart

Universe ratings reflect a weighted average score across two dimensions:

Customer Experience (vertical, y-axis)

- The combined Customer Experience weighted average score across:
  - "Likelihood to recommend" the service provider for security services, and
  - "Quality of security service experience in the past 12 months.
- Experience scores are from an Omdia commissioned, independent primary enterprise customer experience survey of 130 executives. Respondents were screened to ensure each had recent direct experience with a provider before rating them.
- The scores represent the total net of customers awarding high likelihood to recommend (awarded 9 or 10) less detractors (awarded 6 or less).

Overall Solution Capability (horizontal, x-axis)

- The combined capability score of each provider across strategy, innovation, differentiation, breadth, and depth of services in cybersecurity globally.
- Scores were allocated based on Omdia's assessment against a Universe evaluative framework from multiple data points.
- Capability Sources included service provider questionnaire responses, briefings, enterprise customer references, and secondary research through publicly available sources.

Award categories

Market leaders

This category represents service providers with the highest overall ratings across customer experience (vertical-axis) and service provider experience (horizontal-axis).

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Market Leader characteristics include:

- **Customers are strong advocates**
  - Leaders are typically more likely to be recommended by their customers than Challengers and Prospects.
  - Leaders achieved higher-than-average overall customer experience scores from Omdia's independent study in both the "likelihood to recommend" score and their "security service experience" scores.
- **Capabilities are broad, mature, and evolving**
  - CIOs must manage complex cybersecurity needs in large MNCs. Therefore, a Universe leader must have exceptional security service capabilities to meet these needs in more than one area.
  - Leaders excel in three or more service categories across managed services, consulting, threat intelligence, industry services, and technology.
  - Leaders also share a clear strategy, investments, and recent capability improvements in cybersecurity. Examples include talent programs, process, and platforms-led innovation, secure gateways, SASE offers, maturing threat hunting and response automation, new advisory and forensic services, integrated customer dashboards, and customer-led, co-innovated industry best practices.
- **Global capability**
  - Global leaders have significant capabilities across two or more regions, including North America, Europe, and Asia and Oceania.
  - Follow-the-sun capability, 24/7/365, and client proximity with service delivery resources can make or break seamless, effective SecOps and professional services delivery.

Market challengers

This category includes IT security services providers with capabilities and, or customer experience marginally lower than the market leaders.

Market Challenger characteristics include:

- **Customer advocates**
  - Challengers typically achieve an average overall Customer Experience score.
  - Challengers also perform well in one or two particular service categories in "likelihood to recommend" and/or "security service experience."

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

- **Niche market focus**
  - Challengers focus on a particular region that mirrors their parent company's installed base of other services (notably for telcos) or reflects their heritage (e.g., as predominantly a platform company that expanded into services).
  - Challengers do not have the same breadth, depth, or level of experience as Leaders, a function of their focus or time in the market (i.e., they typically excel in one or two of the five service categories (e.g., MSS, Consulting)).
  - Challengers' response to address services breadth, depth, innovation, strategy, and roadmap has been less compelling than Leaders (i.e., each provider engaged with Omdia at different levels of depth, which enabled or limited overall scores for capability, breadth, depth, and expertise).
- **Shortlist candidates**
  - Challengers are nonetheless strong candidates for global IT security services.
  - Each possesses unique capabilities, heritage, expertise, and focus, and this approach makes them viable for MNC customer shortlists.

Market prospects

This category includes providers with IT security services capabilities and/or customer experience lower than the average across the survey. Note that the inclusion standard for this survey was very high, including only the top ten providers.

Market Prospect characteristics include:

- **Maturing Customer advocacy**
  - In the primary research survey, Prospects scored comparatively lower in the overall Peer Recommendation score and fewer service categories than Challengers and Leaders.
- **Emerging capabilities and scale**
  - Prospects are usually newer to the Global IT Security services market.
  - As a result, they have a presence firmly tied to one domestic market and have capabilities in only one or two of the five market definition categories across services breadth, depth, innovation, strategy, and roadmap.

Expanded taxonomy—IT security services

This report assessed and benchmarked the following five categories against their peers.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Table 11: IT security services

Managed security services (MSS)

- MSSPs deliver 24×7 security operations on behalf of customers or as a co-managed shared service supporting internal cyber teams.
- MSSP solutions may range from retainer-based or emergency security incident response services to fully MSS delivered by follow-the-sun and 24×7 SOC capabilities across major customer regions with multilingual capabilities.
- MSS capabilities include security operations services and management of underlying third-party and proprietary security tools, platforms, and software across cloud security (public, private, hybrid, distributed and SaaS), mobile/endpoint, and networks.
- Services are usually delivered directly by the providers in core markets and regional channel partners.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Security consulting, integration, & advisory

- Providers deliver professional services that usually map to the NIST Cybersecurity Framework or similar.
- Examples include consulting and assessments across cyber strategy, cyber-risk and compliance (e.g., GDPR, PCI-DSS, CCPA), adherence to standards (e.g., ISO/IEC 27001, 27013), vulnerability management, ethical hacking and pen-testing, forensics, data governance, zero trust, identity management, DevSecOps, security architecture, cloud security maturity, staff security awareness, and organizational training.
- Emerging services include CISO/CIO as a service, giving customers access to on-demand cyber experts in their local language on cyber issues from strategy to ongoing SOC and operations.
- Mature providers offer security capabilities supporting broader digital transformation agendas across strategy, design, implementation and cyber operations in complex, large-scale organizations.

Threat detection & intelligence

- Proactively helps organizations assess, detect, and respond to threats across IT and OT environments through tools, platforms, analytics, automation, and security staff expertise.
- Threat intelligence usually includes access to proprietary and third-party threat telemetry and intelligence enriched by User and Entity Behavior Analytics (UEBA) and continual threat hunting.
- Services delivery is through a combination of global threat databases, alerts, feeds, portals, platforms, automation, playbooks, and AI and SOC analysis, accessible through a single pane of glass.
- Managed Threat Detection and Response is a growing area in this category, usually targeting smaller organizations with less mature cyber operations capabilities.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Industry cybersecurity solutions

- Industry-specific and sector-tailored cybersecurity across consulting, advisory, and managed services.
- Providers assemble consulting, advisory, threat intelligence, and MSS to address sector-specific challenges (e.g., IoT security for manufacturing, supply chain, and logistics).
- Services are often an overlay, service package, or additional domain of cyber expertise that reflect the unique value chain and ever-changing regulatory, governance, risk, and compliance landscape each sector faces.

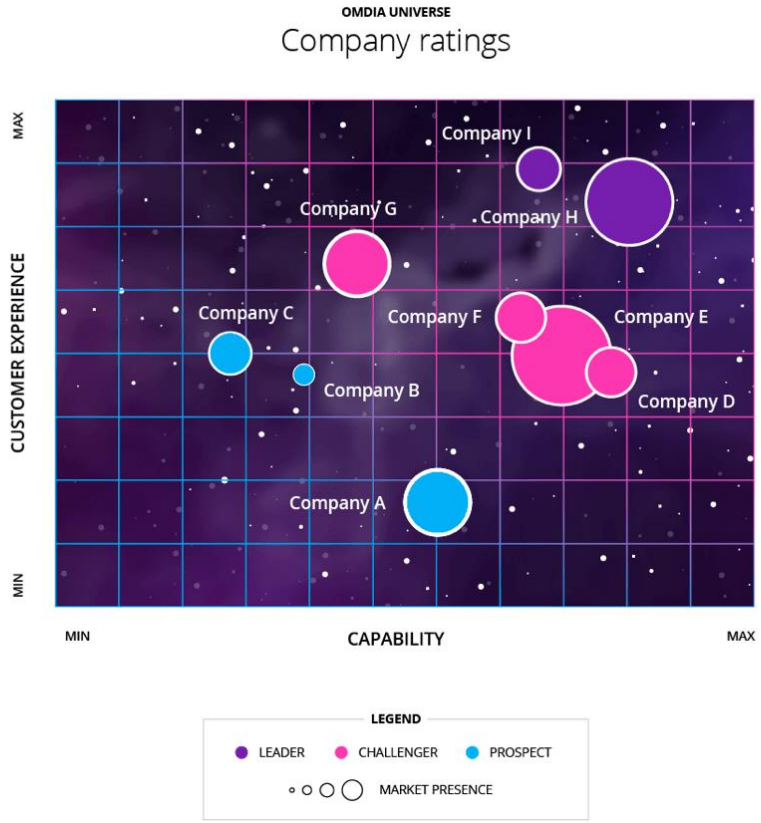
Cybersecurity technology & software

- Providers are a channel to market for leading security software and platform providers.
- Providers are value-added resellers (VAR) of proprietary, third-party service management, SaaS and security software, appliances, hardware, or cloud-based security capabilities delivered through on-premises appliances, software, or cloud-based solutions.
- Services span security information and event management (SIEM) platform capabilities (cloud or on-premises), endpoint and mobile (agent-based) security software, next-generation firewalls (NGFW, including IPS and DPI), cloud security (incl. workloads and containers), SD-WAN, edge, mobility, and IoT.
- Vendor examples include Amazon, Alibaba, Avast, CA, Carbon Black, Checkpoint, Cisco, Cloudflare, CrowdStrike, Fortinet, F5, Fire Eye, IBM, Jira, McAfee, Microsoft, Okta, OpenText, Palo Alto, Qualys, ServiceNow, Sophos, Sentinel One, Splunk, Symantec, Tenable, VMware Carbon Black, Zscaler.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Interpreting the Omdia Universe chart

Figure 15: Omdia Universe



Source: Omdia

Capability (x-axis)

- IT service provider (ITSP) security capabilities were assessed across each of the five IT security service categories (A) against five benchmark measures (B).
- The weighted average determined the overall score.
- These scores also reflect the “solution capability” in each vendor radar chart.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Benchmark measures per service

Table 12: Benchmark measures per service

Strategy & roadmap includes:

- ITSP offered a compelling 12-month to three-year vision and strategy from the perspective of multiple stakeholders, including one or more C suite, IT managers, SOC teams, and ecosystem partners.
- Roadmaps and strategy weave together capabilities across service types and industries, including complementary technologies such as cloud and AI/ML, to address large enterprise and government needs.

Innovation includes:

- Proprietary tools, playbooks, and patents driving advances in threat intelligence platforms and services.
- Globally and regionally available, established centers of excellence in cyber, including co-creation with clients and partners.
- Customer experience driven user-friendly dashboards/digital experiences (e.g., board level and SecOps/MSS SOC console-level across services and technologies.
- Market differentiation includes:
- Brand awareness, reputation, and market presence globally and within regions.
- Multiple, clear, compelling customer perspectives from interviews, case studies, and confidential references.
- Evidence of thought leadership from reports, articles, threat attribution, and security event participation.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

The breadth of services includes:

- The comprehensiveness within and degree of integration across each service category:
  - **MSS:** From SOC as a Service, incident retainer, or emergency services to fully outsourced.
  - **Threat:** Threat intelligence portals, API/XML feeds through standalone, fully managed, proactive threat hunting and intelligence services.
  - **Consulting:** Standalone consulting and advisory in IT Security Strategy and Governance from the Boardroom to SecOps.

Depth of services includes:

- The level of expertise and demonstrated ability within each service category across each region and industry:
  - **MSS:** number of SOCs, qualified and certified staff, industry certifications and accreditations (e.g., cloud MSSP partners), well-defined publicly available service descriptions, legal terms and SLAs, client examples/wins, platform and service integrations.
  - **Consulting:** Specific reference security-specific C&SI capabilities, skills, people, or expertise available to clients globally.
  - **Industry:** Demonstrated industry-specific security capabilities in targeted verticals, co-creation of security solutions (e.g., IoT), recent customer wins, and thought leadership in sector security challenges.

Experience (y-axis)

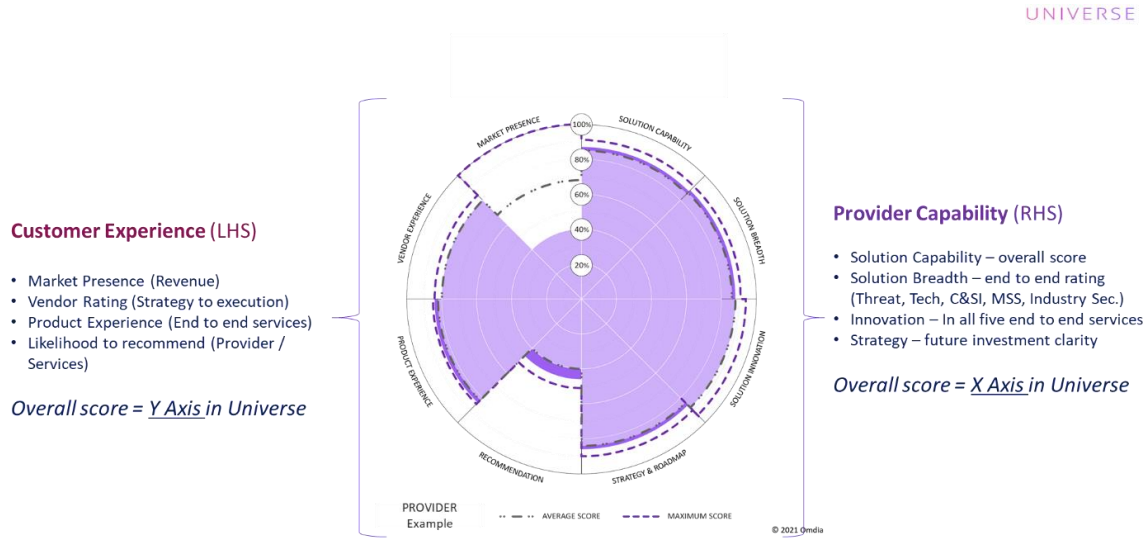
- The Customer Experience Score (CX) score is the weighted average of the "likelihood to recommend" and "service provider experience" scores in IT security from an Omdia commissioned primary research survey conducted in 2Q22 of senior IT decision-makers at large enterprises and governments.
- Several service providers also provided direct references, which uplifted CX scores in some services, referenced in vendor assessment analysis.

Understanding the Vendor Radar

Chart results for each service provider compared to the average and the maximum across each category:

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 16: Vendor radar guide



Source: Omdia

IT Security Services Universe inclusion criteria

- **End-to-end security services:** Offer IT security services across all five categories: MSS; security consulting & integration; threat detection & intelligence; security industry services; and security technology services.
- **Global:** Have a demonstrable depth of capability and market presence within and across survey target regions, principally Asia and Oceania, EMEA, and North America.
- **Market presence**: Serve at least 500 large enterprise and government customers, with their base spread across all major regions globally. Providers attribute significant global revenue from IT/cybersecurity services (i.e., more than $500m annually) and have an evident focus on IT security.

Assumptions

Focus on large multinational corporations (MNCs), governments and large enterprises

- This report focuses on the holistic security buyer needs of the Fortune 500 type MNCs, and governments. Future editions may explore the mid-market (circa 500–2,500 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 and Latin America and the Caribbean.

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Score calibration

- In all cases, the Omdia assessment best uses publicly available material, analyst assessments, and analyst briefings.
- All ratings, vendor analysis, and the Omdia Universe report have been through 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, Kyndryl, IBM, and NTT declined to participate in this edition, and BT and DXC provided limited input.
- Participating providers supplied confidential sources under NDA, used in the benchmarking scores.
- Many providers could not disclose regional revenue splits due to company policy. Revenue numbers are Omdia estimates.

Additional service providers

Due to this report's breadth and inclusion criteria, several alternative IT security services providers are not included in this edition of the Universe. Noteworthy service providers Omdia analysts monitor include:

- Arctic Wolf
- Atos
- Capgemini
- Deloitte
- Fujitsu
- HCL Technologies
- Lumen (formerly CenturyLink)

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

- Infosys
- TCS
- Trustwave
- Wipro

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Appendix

Further reading

Service Provider Spotlight: Kyndryl Takes a Bow on Global Managed Services Stage with New Opportunities Waiting (January 2022)

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

Digital Enterprise Services Insights: Global Cybersecurity Services (Cloud, Edge, MSSP) 2021–22 (August 2021)

Digital Enterprise Services Insights: Global Cybersecurity Market Landscape – 2021–22 (May 2021)

Enterprise Services Total Addressable Market Forecast: 2020–26 (September 2021)

Cybersecurity IT Services Contracts Analysis: Global – 2021 (April 2021)

"Service Provider Spotlight: BT Signals Global Security Ambitions with Eagle-i" (November 2021)

Global Security Services Forecast 2020–25: Cybersecurity – the cornerstone of digital resilience (December 2020)

Author

Adam Etherington, Principal Analyst, Digital Enterprise Services

askananalyst@omdia.com

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.

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

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") 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 and agents, 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

omdia.com

askananalyst@omdia.com

© 2022 Omdia. All rights reserved. Unauthorized reproduction prohibited.