OMDIA UNIVERSE

Publication date
18 March 2021

Author
Adam Etherington
Principal Analyst

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

OMDIA

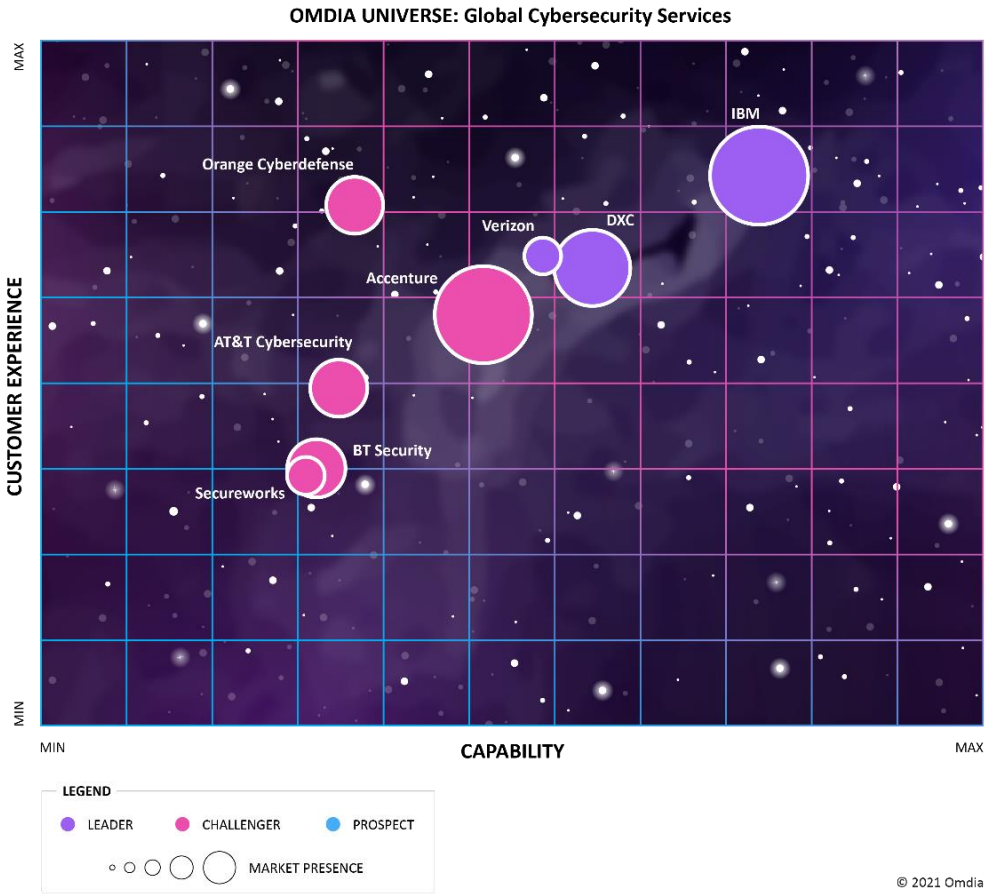
Brought to you by Informa Tech

Summary

Catalyst

This Universe offers an independent, comprehensive, end-to-end assessment of world-leading global IT security service providers across two major IT security dimensions: end-to-end service capability and customer experience, and will assist decision-makers in shortlisting providers best suited to their requirements. DXC, IBM, Verizon are market leaders, scoring exceptionally well across both customer experience and service capability dimensions.

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



Source: Omdia

Omdia view

Organizations globally were already moving to digital enterprise services, and the COVID-19 pandemic accelerated this shift. Firms of all sizes, within all sectors, quickly moved to enable core business resilience under different market conditions, mobilizing employees and their applications to work remotely, needing flexibility in scale and OPEX as financial conditions deteriorated or pockets of growth arose. These shifts toward digital are permanent, and firms have continued to rely on

technology to maintain core business operations. Besides creating new options, enterprises are preparing themselves for future innovation as the world returns to growth.

Cybersecurity presents a growing challenge to meet these objectives on many fronts. One is resultant IT sprawl, and increasingly complex information and communications technology (ICT) ecosystems. The rapid shift to digital by firms in response to COVID-19 has resulted in broader attack surface areas. Further, Omdia observes increasingly sophisticated threats by motivated and well-equipped adversaries including organized criminal groups and nation states. Budget constraints from the economic downturn did not ease the global skills shortage. There was no slack in demand for experts who can mitigate risks effectively.

Global Cybersecurity service providers are vital in this landscape, delivering organizations different combinations of capabilities across industries, geographies, and IT security domains to address current and emerging threats. These service providers partner with large organizations to navigate complex IT security challenges. Each has unique combinations of skills, industry experience, market commitment, innovation, breadth, and depth of services across security-specific domains; threat intelligence, consulting, integration, technology, industry services, and managed services.

Key messages

- In this inaugural report on IT managed security services, IBM is the clear market leader, excelling in breadth, depth, and customer experience globally for large enterprises and government organizations.
- DXC and Verizon are classified as leaders, achieving the next highest overall ratings on customer experience and service capability across three or more security service market categories.
- AT&T, Accenture, BT, Orange, and Secureworks are market challengers. All offer a comprehensive suite of IT security services.
- The challengers' degree of service capability, customer experience, and product integration is not as substantial as the market leaders'; however, they are by no means laggards, each excelling in different aspects of IT security.
- The global telcos that have invested heavily in security are rapidly maturing. They are focusing on end-to-end capability, offering integrated services, deepening industry capability, and leveraging their sizable customer base from network services.
- Most providers are investing in the next generation of managed security including managed threat detection and response (named XDR by Omdia, MTDR and MDR by others), machine learning and artificial intelligence, security orchestration and automation, and cloud security.
- Omdia qualified leading providers for participation in this report based on factors including services capability and enterprise feedback. Inclusion in the Universe itself is an accolade.

Analyzing the Global IT Security Services Universe

How to use this report

Omdia advocates the business benefits that can be derived from technology, including digital transformation, business resilience, and innovation. IT security services are the cornerstone of realizing digital transformation, business resilience, and innovation in a world disrupted. This report provides an independent assessment of major global IT security service providers. All those assessed differ in degree of capability across all aspects of service capability and customer experience.

Cybersecurity is complex. CIOs and CISOs alike must consider a suite of capabilities to secure and enable their respective enterprises. To address this complexity the evaluative criteria in this report cover all major IT security domains, not just managed services. This inaugural report addresses the breadth of capability required for useful comparisons.

For enterprises, Omdia Universe guides and informs the selection process to match provider capability to enterprise need. For service providers, this report highlights opportunities and market perceptions to consider in roadmaps, partnering, product management, and market positioning.

Market definition

This Universe is global in scale and wide in its breadth of capabilities assessment. This sets it apart from comparative studies that only focus on one category (e.g., managed security services).

This Omdia Universe evaluates global security service providers that help organizations manage the confidentiality, integrity, and availability (CIA) of ICT The CIA triumvirate is at the core of information security. Service types to achieve this span consulting, design, build, and manage; hardware, software, and cloud-delivered models; and standalone and integrated security services.

Omdia's research confirms most large enterprises have, on average, at least two major providers of security solutions or individual services, spanning from relatively mature services (e.g., managed firewall) through to turnkey, bespoke, and fully customized consulting engagements. Further, services are nuanced to meet local market restrictions and industry client's needs.

Each provider uses different terms for comparable services. Omdia has defined the following five categories for comparison in this Omdia Universe to capture the most critical capabilities across those surveyed to deliver large enterprise and government client needs.

- **Managed Security Services.** Reactive and proactive managed IT security services, including remote monitoring, device management, and patching of devices, applications, cloud services, and enterprise sites. Common examples include Managed Intrusion Detection System/Intrusion Prevention System (IDS/IPS), firewalls, web gateways, Security Information and Event Management (SIEM), Security Operations Center (SOC) and Computer Emergency Response Team (CERT), SOC-as-a-service, Managed Detection and Response (MDR), Security Orchestration Automation and Response (SOAR), ongoing support services under retainer, and others.

- **Security Consulting and Integration.** Security specific advisory and professional services from the boardroom to operations. Common examples include crisis response and forensics; penetration testing; security strategy, assurance, and governance, risk, compliance (GRC) consulting; security architecture and design implementation; and integration and deployment services.

- **Threat Detection and Intelligence.** Threat research, gathering, synthesis, curating, analyzing reporting, feeds, alerts, and actionable intelligence; enterprise access to proprietary and third-party feeds, augmented by artificial intelligence (supervised and unsupervised machine learning techniques); enterprise telemetry gathering, analysis, and assessments; mature providers integrate threat intelligence with managed services to address sector-specific threats.

- **Security Industry Services.** Unique combinations of managed and professional services that are distinctly addressing sector-specific Cybersecurity challenges. Examples include bridging physical with Cybersecurity in 5G, the Internet of Things (IoT), and Industrial IoT (IIoT) in manufacturing and energy sectors, or cyber risk management and financial services compliance.

- **Security Technology Services.** Often includes the resale of third-party vendor software or hardware solutions and deployment across one or more areas, including infrastructure, cloud, SD-WAN, edge, mobility, IoT, big data, enterprise applications, digital tools/engagements. Organizations may then manage it in house or onboard to a managed service.

Omdia Ratings

Universe ratings and chart position reflect a weighted average score across both customer experience and service provider experience dimensions. Scores were allocated based on Omdia's assessment against a Universe evaluative framework. Sources of information for rating and scoring included service provider questionnaires and briefings, a primary enterprise customer experience survey, enterprise customer references, secondary research through publicly available sources, and an internal peer review process with Omdia's relevant analyst subject matter experts.

Market leaders

This category represents service providers that achieved the highest overall ratings on customer experience and service provider experience dimensions across the Universe.

Leaders received the highest relative peer recommendation scores. Leaders also typically achieved higher overall customer experience scores, and had high relative customer ratings across vendor experience, product (security service) experience, and general advocacy (peer recommendation).

Leaders in security service capability excelled in multiple service categories (e.g., managed security, industry security), spanning breadth, depth, innovation, strategy, and roadmap.

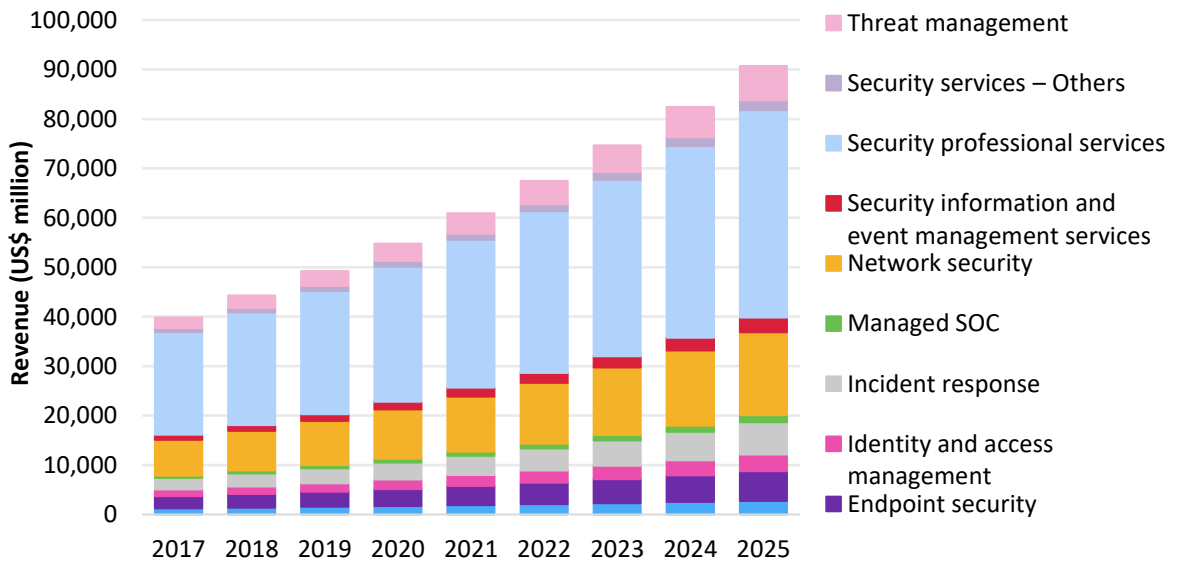
Market challengers

Challengers, by no means laggards, excel in aspects of cybersecurity. They possess scale and demonstrated competency and proficiency, making them suitable for customer shortlists and meeting requirements of most multinational enterprise and large government customers. Challengers excel in services breadth, depth, innovation, strategy, and roadmap in Cybersecurity, between one and three of the five market definition categories.

Market Outlook

Omdia forecasts the global cybersecurity services market will reach $91 billion by 2025, a CAGR of 10.6% over the 2020–25 period. IT Security has accelerated as a spending priority. It is among the fastest addressable services growth markets, behind cloud (19% CAGR) and emerging services such as artificial intelligence and blockchain (39% CAGR). **Figure 2 shows** various elements that comprise the global cybersecurity market.

Figure 2: Global cybersecurity market, 2017–25



Source: Global Security Services Forecast 2017–25: Cybersecurity—the cornerstone of digital resilience

- **Growth areas**: The fastest-growing managed security services markets out to 2025 are:
  - threat management services that address the increasing volume, sophistication, and cost of data breaches (14.4% CAGR),
  - managed security information and event management (SIEM) services (14% CAGR) to contend with increasingly sophisticated telemetry,
  - incident response services (13.7%), which help organizations respond quicker.
- **Size of spending**: The largest addressable markets by total spend remains professional security services (9% CAGR); network security (11% CAGR) including remote management; and incident response (13.7%).
- **COVID-19 impact**: Omdia's cybersecurity forecast considers the implications of COVID-19, which shaves approximately 4% of total growth in 2020-25. Omdia estimates that spending stagnated in the largest subsegment, security-specific professional services, as enterprise austerity measures swiftly kicked in, reducing OpEx wherever possible to buffer profit margins during the prolonged downturn.

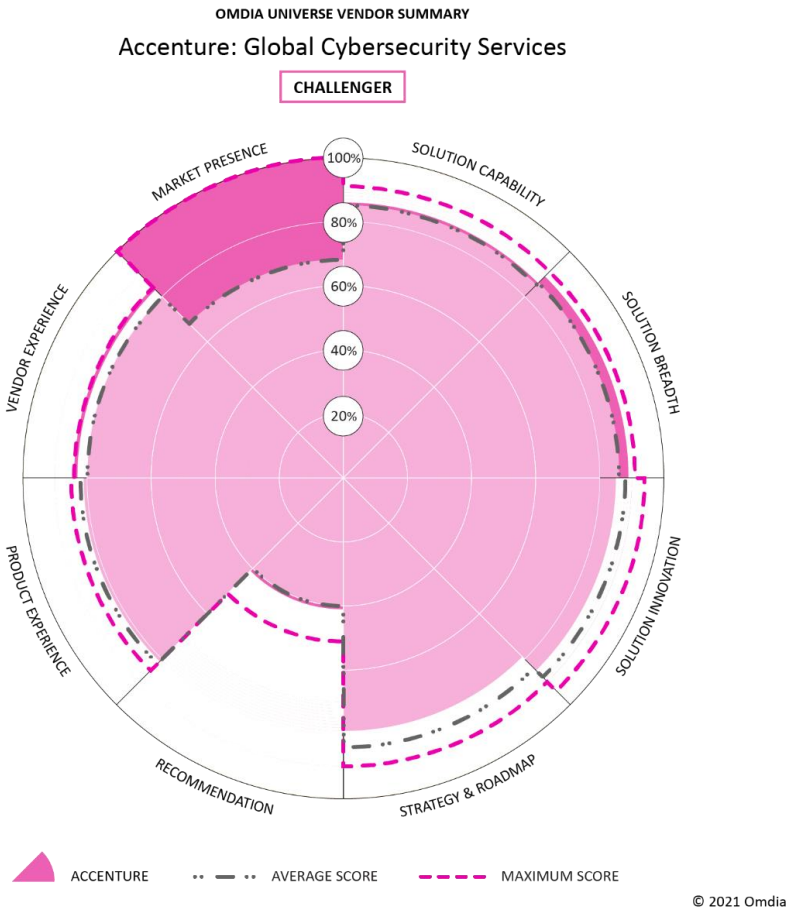
Service Provider Analysis

Accenture (Omdia recommendation: Challenger)

Accenture should appear on shortlists of enterprises that need global scale, consulting and advisory services breadth, and a cloud focus.

Omdia views Accenture as a significant challenger in IT security services. Omdia estimates the provider has amassed a large market presence and significant global cybersecurity revenues.

Figure 3: Omdia Universe ratings: Accenture



Source: Omdia

The company achieved above-average security services breadth scores because of deep industry and management consulting experience applied to enterprises' cybersecurity challenges.

Service Provider Summary

Accenture's security services sit within the company's Technology Group, alongside complementary capabilities including cloud, systems integration and application management, platform, infrastructure and software engineering services, data, and artificial intelligence.

The company's sizeable security strategy and consulting capabilities reflect a historical focus on Technology and industry strategy interaction and strongly complement Accenture's managed security services.
While dominant in North America, representing ~50% of global revenue, Accenture also has a considerable presence in Europe (~30% revenue) and "growth markets," including APAC (~20% revenue).

Universe Assessment

Accenture's strengths include comprehensive security services breadth complemented by management consulting and industry experience, global scale, and a market presence accelerated by acquisitions.
Accenture received a peer recommendation score of +41 across global surveyed customers, ranking fifth among Universe peers. Customers are firm advocates of Accenture's Threat Intelligence and Consulting and degree of cybersecurity service capability.

Accenture has excellent service breadth and ample opportunities to position IT security services. The provider has established deep relationships across C-suite executive. Omdia notes that non-IT decision makers and influencers increasingly influence security spending. Accenture also has significant market presence achieved through organic growth and many acquisitions globally.

Accenture's security services portfolio is comparatively broad. Services span managed security (application, cloud, digital identity, risk, and threat management), industry security (OT/IIoT/ICS, strategy/risk, and deep industry expertise, e.g., border management), cyber defense (threat intelligence, application security, advisory, forensics, and operational readiness advisory), and applied cybersecurity (infrastructure and cloud, data, identity, risk management/GRC, and platform security).

Accenture has far reaching expertise that it can leverage. The company's established experience with management consulting and business strategy, change management, and technology innovation, is complemented by extensive IT outsourcing and systems integration capabilities. Further, Accenture has the industry expertise and a multi-sector approach that sets it apart from other security service providers, leveraging global "Cyber Fusion Centers" to drive client innovation. Technology capabilities are enhanced by strong alliances with Palo Alto Networks, Amazon Web Services (AWS), ServiceNow, and other vendors, complementing its depth and degree of client innovation potential in security.

Accenture has established global customer base to leverage. Accenture has an established global customer base, including 91 of the Fortune Global 100 and three-quarters of the Fortune Global 500.

The company provides services across 40 industries with operations in over 200 cities and 51 countries.

Acquisitions have strengthened depth, breadth, and reach. The recent acquisition of Symantec's Cyber Security Services business from Broadcom augmented Accenture's IT security service depth and added global scale. The investment added six security operations centers (SOCs) located in the US, the UK, India, Australia, Singapore, and Japan. Accenture also added Symantec's proprietary cloud-based platform for technical and cyber adversary threat intelligence.

Accenture continues to make smaller, tactical acquisitions in security. For example, Revolutionary Security Context (IT and OT security), Information Security (enterprise apps and IoT), Deja Vu Security (enterprise apps and IoT), iDefense (VeriSign's intelligence services), Maglan (APAC market presence), Redcore (APAC market presence), Arismore (IAM), and FusionX (advanced cyber threats).

"**Cloud First" will strengthen security capability and differentiation.** The formation of Accenture's "Cloud First" multi-service group will help the company capture the growing cloud-based security market. Accenture announced continued investment (~$3bn) in cloud capabilities. This is a bold and precise play to lead across strategy, migration, optimization management and security in enterprise cloud. This strategy will enable Accenture to capitalize on the continued shift of critical workloads to hybrid cloud infrastructures and underlying security concerns.

Accenture's opportunities and threats include leveraging acquisitions within a clear cybersecurity vision and enhancing managed services and threat intelligence differentiation.

Nurture advocates in managed security and technology. Accenture's customer satisfaction ratings were very positive (averaging 8/10) but lower relative to other providers in this Universe. Both in managed security services and technology services capability, and customers' perceived degree of security innovation or breadth of Accenture security services.

Promote a cloud centric security strategy. There has been no shortage of recent announcements of Accenture's acquisitions across cloud, security, and other areas. The aggressive acquisition strategy presents a formula for Accenture to build a clear vision for integrated security. Omdia recommends Accenture clearly showing customers how these investments complement the providers security services. Especially linking new capabilities with Accenture's existing deep industry and consulting expertise and mature partnerships.

Explore repeatable integrated security services. Accenture's consulting-led approach emphasizes custom solutions as part of its integration, technology refresh, and transformation. Global large enterprises are reeling at the complexity of securing complex, sprawling IT estates within budget constraints. Omdia believes there is a market opportunity for repeatable, customizable but non-bespoke, integrated security solutions with flexible price points for different industries that Accenture could explore. For example, other telcos in this Universe are investing heaving in customer journey led security offerings that integrate common service elements across sectors.

Facing stiff competition. Accenture faces rigorous competition from specialized security providers, global telcos with credibility executing cost-effective network transformation, other extensive

systems integrator and outsourcing providers targeting Accenture's global customer base, and from providers exploring innovative product constructs, going to market through new channel models.

AT&T Cybersecurity (Omdia recommendation: Challenger)

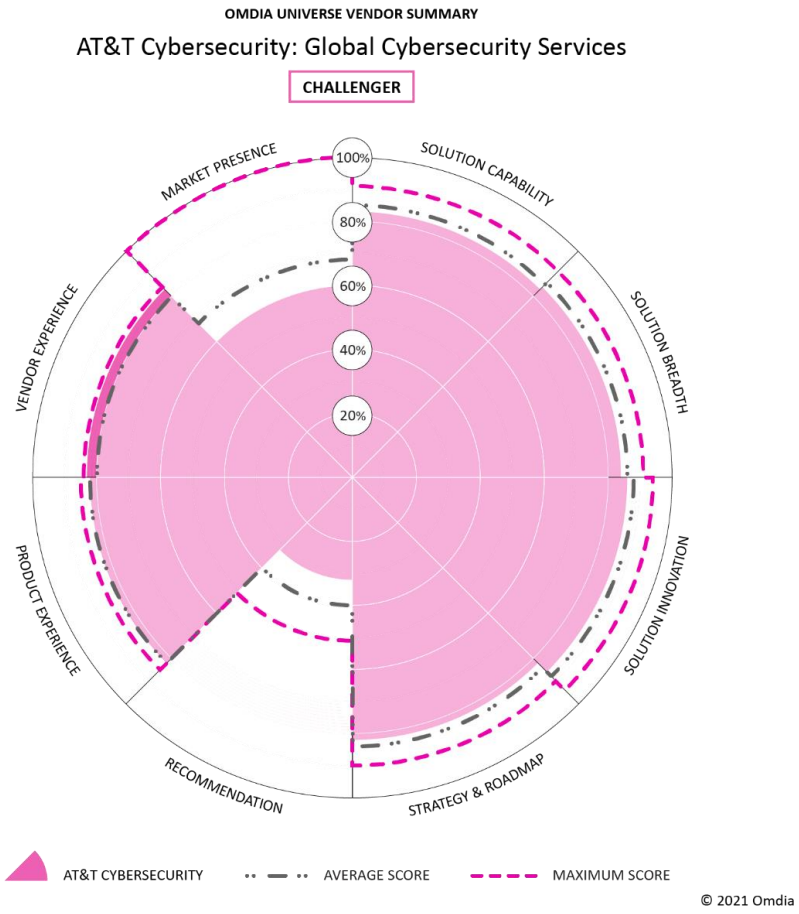
AT&T Cybersecurity should appear on shortlists for enterprises that seek global scale in managed network security, network transformation, and deep threat intelligence capability.

Omdia views AT&T's Cybersecurity division as a robust challenger in global IT security services. The company has excellent services breadth from a long history in telco security, augmented by its acquisition of AlienVault.

Inked in 2018, the investment of the privately held company added a threat intelligence unit and access to a unified security management software platform. These acquired capabilities are now firmly integrated within AT&T Cybersecurity as Alien Labs™ and AT&T Unified Security Management (USM)™ respectively.

Surveyed customers rated AT&T highly in vendor experience, primarily in the degree of security innovation, vendor experience in security, and security service capability. AT&T's managed services product experience was also rated highly.

Figure 4: Omdia Universe ratings: AT&T Cybersecurity



Source: Omdia

Service Provider Summary

AT&T Cybersecurity is the IT security division for AT&T Business. The company is the largest incumbent telco in North America, and has a sizeable presence in EMEA, APAC, and Latin America. AT&T is the world's oldest telephone company in operation, spanning 140+ years. The company has longstanding experience managing complex fixed and mobile network security. AT&T supports clients through eight Global SOC's and over 2,000 security professionals. AT&T's security threat intelligence is enriched by its development and support of the Open Threat Exchange, a crowd sourced security platform recognizing over 20 million threats daily submitted by ~168,000 security professional members.

Universe Assessment

AT&T Cybersecurity strengths include Managed Security Platform and Threat Intelligence capabilities following its AlienVault acquisition, a longstanding, global scale in network management, and an integrated Managed Threat Detection and Response service.

Customers are advocates of AT&T managed security and vendor experience in security. AT&T achieved a peer recommendation score of +32, ranking sixth among Universe peers, and ranked second overall in vendor experience. Customers scored AT&T highly across all categories, including the degree of cybersecurity innovation, vendor experience in security, security service capability, breadth, and strategy and roadmap. In product experience, customers are the strongest advocates of AT&T's managed security services.

A security division bolstered by acquisition. AT&T Cybersecurity is the security division within AT&T Business which gives it market focus and presence. This asset mix and organizational structure enables integration across security services and a coherent strategy. AT&T also owns and operates one of the world's largest fixed and mobile networks. The AlienVault acquisition combined with AT&T Managed and Consulting Services, enabled a step-change in security capability and revenue. AT&T's platform and threat intelligence capability includes AT&T Alien Labs™ threat intelligence and AT&T Alien Labs Open Threat Exchange™, which supplies threat intelligence feeds both for AT&T and for the company's security peers and competitors.

Network security heritage. AT&T's heritage brings credibility to its network security services. Within the company's operations, the Alien Labs division collaborates closely with the AT&T Chief Security Office and AT&T's global SOCs to enrich its telemetry data and intelligence. The cybersecurity division leverages AT&T's global scale in network management and operations security. The evolving fixed and mobile network convergence, industry use cases, and the promise of 5G creates opportunities and challenges for firms.

Integrated security services building on USM. Integration of the AT&T Unified Security Management, (AT&T USM) platform into AT&T Managed Security Services enables the company to integrate, process, analyze and manage large volumes of complex threat intelligence. For example, the AT&T Managed Threat Detection and Response (MTDR) service continuously monitors customer environments through the AT&T Unified Security Management Platform, including orchestration across AT&T AlienApps™ and AT&T Managed Security Services. While some service providers' MDR services are limited to a particular endpoint and on-premise physical or virtualized devices, the AT&T service spans a broad attack surface, including major SaaS providers (Office 365, G Suite, Okta, Box, ServiceNow, and Salesforce), and IaaS (AWS, Azure, GCP). AlienApps™ is vendor agnostic. In 2020, AT&T developed approximately 20 new threat detection and security orchestration capabilities, including Fortinet, DDI, MobileIron, and SentinelOne.

Clear Industry Security services. AT&T is relatively mature for a telco, with sector-specific use cases, intellectual property, and demonstrated experience through case studies and insights. AT&T Cybersecurity links to the company's many other underlying, network-related capabilities.

AT&T's opportunities and threats include lifting customer advocacy, extending market presence beyond the network, and leveraging industry-specific cybersecurity expertise.

Elevate overall advocacy through customer awareness of consulting and industry solutions. Relatively lower product experience scores than Universe peers limited the overall leadership standing. Notably customer security service experience ratings of industry solutions and security consulting integration services. AT&T has perceived strengths that can be leveraged. Customers rated the company relatively high in overall vendor experience across innovation, vendor experience, and service capability.

Stand apart, beyond the network. Telcos are often painted with the same brush and are not always high on the awareness or consideration set for security-centric consulting, integration, or industry solutions outside the network. Further, in managed IT security services AT&T faces stiff competition from all sides. Its competition includes other providers in the North American market, global systems integrators (SIs) and IT outsourcers with in-depth consulting and industry expertise, and regional competitors out of Europe and APAC offering breadth, depth, or nuanced local services.

Drive industry security. As virtualization and the shift to cloud-enabled business models continue to accelerate, and the importance of security around 5G and edge increases, AT&T's capabilities present a growth opportunity. The company should look to grow in-market awareness and credibility across: USM services; industry services beyond those it has already established in and retail and healthcare; more tightly integrated, proactive MDR security services; and further integration of extensive telemetry data with Alien Labs threat intelligence. AT&T can play to its strengths by emphasizing its perceived service strength in security consulting, network integration, and industry services. Emphasizing these strengths would likely drive up AT&T's overall peer recommendation improvement.

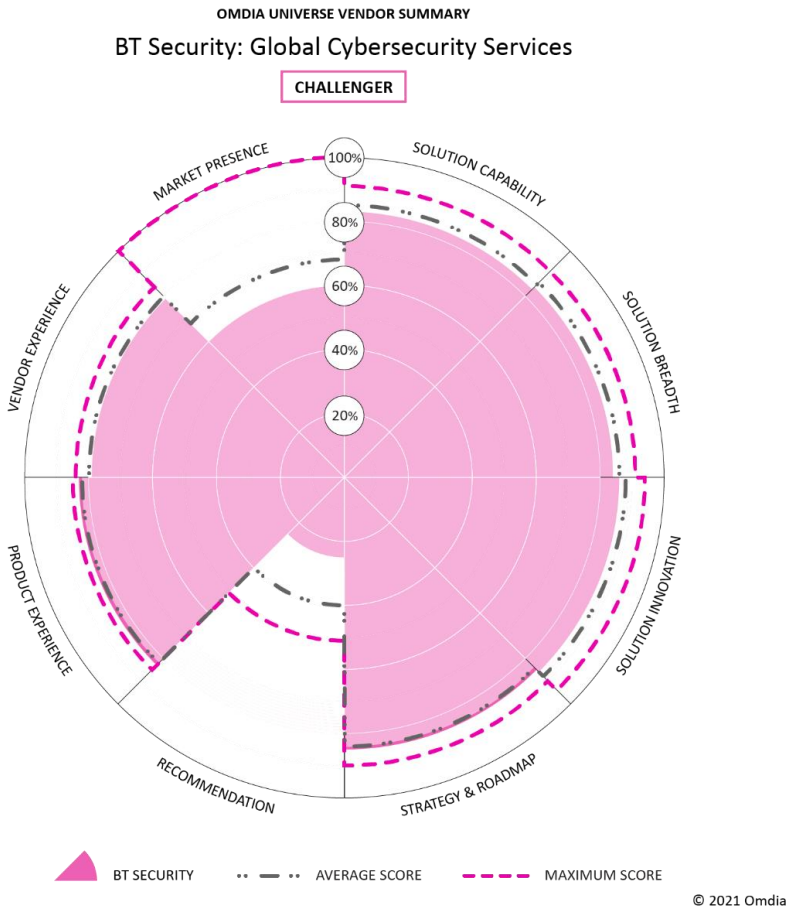
BT (Omdia recommendation: Challenger)

BT should appear on your shortlist if you value a telco with emerging productized end-to-end security services capabilities mapped to customer journeys.

Omdia views BT as a rising star in global IT security services. The company has a compelling growth strategy, vision, and roadmap that makes the most of their network experience—offering clients holistic security services that are more customer journey driven than technology-centric.

Surveyed customers rated BT highly in the degree of security innovation and experience with their security industry services.

Figure 5: Omdia Universe ratings: BT Security



Source: Omdia

Service Provider Summary

BT Security is a fast-growing division within the UK-based £22.82bn BT Group. The company has a substantial UK presence with 85% of BT Group revenue (including Enterprise, Consumer, Global, and Openreach) from UK customers: EMEA at 8%, Americas at 4%, and APAC at 3% make up the group's total revenue balance. Global security services revenues have risen consistently year-on-year to achieve a sizeable market presence. BT's global scale is proliferating as the company adds more security customers from its MNC telco base. BT supports clients through 16 global Cyber Secure Operation Centers, over 3,000 security professionals, invests ~£62m annually in security research and development, and has assembled a broad set of IT security capabilities.

Universe Assessment

BT's strengths include winning customer confidence as demonstrated by sustained organic market growth, growing scale, a compelling vision, and innovative security services.

Customers are advocates of BT's industry security. In advocacy, surveyed customers rated BT's security industry service experience as very high, as was BT's demonstrated degree of cybersecurity innovation. BT achieved a peer recommendation score of +25, doing well in absolute terms. Ranking eighth among the high bar set by other Universe providers assessed.

Impressive organic growth. BT has amassed significant security-specific revenue, doubling its market presence through continued organic growth—an impressive increase in a market dominated by acquisitive growth.

Recent growth involved assembling a comprehensive and coherent portfolio in a complex market through bespoke deals, leveraging a newly minted portfolio of security offers and capabilities. Responding to the rapid shift in security needs caused by the recent pandemic, BT Security launched 12 headline offers. These included threat advisory, hunting, and managed services.

The company has won market confidence, added prominent new logos, and secured renewals in most major sectors. Its target industries include banking, transportation, manufacturing, and utilities.

Investing in scale. The company continues to grow scale in support of a large customer base. BT Global is opening a new cybersecurity operations centre (SOC) in Paris and has upgraded existing SOC facilities in Madrid and Frankfurt. BT also launched a Security Advisory Services practice to offer strategic security guidance and services, which have been resonating with customers.

A compelling roadmap. The company has a clear strategy for continued security growth. BT is committed to lifting security services revenue to £1bn by 2023/24 through a targeted growth phase commencing 2Q21. Omdia believes that the telcos' challenge in security services is to transform the business from network-led to digital services led. BT's is addressing the challenge by concentrating on the link between business outcomes, the customer journeys to realize them, and security challenges from BT's industry experience. Instead of focusing on technology first, BT leverages its telco bundling experience, emphasizing straightforward client security propositions underpinned by service innovation.

User story led product innovation. A good example of such a client security proposition is BT's "Graded Service Model." Enterprises can find the breadth of IT security services and products to be overwhelming. BT is seeking to address this with a standard set of pricing, graded in "foundation," "foundation plus," and "premium" levels, built on scalable and repeatable integrated security. These graded offers will span advisory, onboarding deployment, monitoring and management, and continuous improvement within selected customer journeys or scenarios (e.g., Hybrid Cloud and monitoring and remediation across OT environments).

BT's opportunities and threats include increasing brand awareness of security capabilities, especially outside the UK, and building industry credibility with unique sector-specific security offers enabled by its Graded Service Model and new Eagle-i platform.

Elevate BT security customer awareness. In advocacy, BT has some work to do. The company's level of awareness amongst global enterprises, vendor experience, and security service breadth was very positive, but lower than Universe peers.

BT's capabilities are growing, and the company has added some excellent client references. Both are assets in lifting peer recommendation. Omdia also believes that BT should better communicate its client roadmap and elevate its brand presence in North America, EMEA, and APAC through industry offers and the Graded Service Model, alongside client references. These factors may help lift customers' impressions of BT's security services.

Increase industry focus within products. Building and promoting sector specific security services is advised to address industry requirements. BT has organized global sales and marketing teams across industry segments, supported by a worldwide campaign a large customer base across major sectors. However, BT faces robust competition from other providers that build and actively promote integrated security service product and offers into target industries.

Lead OTT security. Another opportunity for BT is to execute on the BT Global Division's new over-the-top (OTT) digital platform plays. In September 2020, BT announced it had deployed a new IT stack, through which customers could consume BT's network and hybrid cloud services alongside third-party software and services. "Eagle-i" is the security-specific variant of these new operations, offering managed security services based on best-of-breed partners.

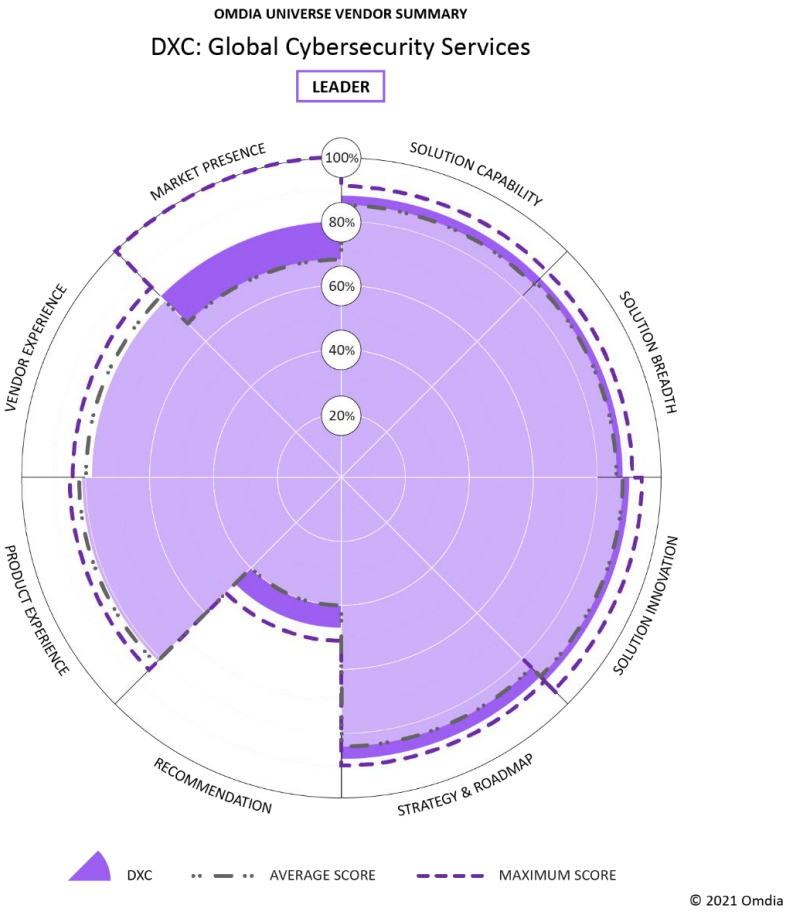
Continue to innovate. BT's Graded Service Model, "Eagle-i" portfolio integration, and a healthy list of reference customers, should resonate well with the market. The new ThreatCo platform may help address some of the complexity in the security market and BT can back its expertise through relevant industry use cases.

DXC (Omdia recommendation: Leader)

DXC should appear on shortlists for enterprises that value an established global provider with systems integration, enterprise application, hybrid cloud, and outsourcing related security experience.

DXC achieved a leadership position in this IT security services Universe. The company has a global presence spanning all major regions and broad service capability, matched with depth of security expertise, a deep partner ecosystem, a high degree of service flexibility. The company also achieved the third highest peer recommendation score among tracked competitors.

Figure 6: Omdia Universe ratings: DXC



Source: Omdia

Service Provider Summary

DXC Technology resulted from the merger of CSC with HP Enterprise Services, designed to better support customers by industry, across the "Enterprise Technology Stack." IT security sits within the company's largest division, Global Infrastructure Services (GIS), alongside IT Outsourcing, Workplace Solutions, and Cloud.

The provider's capabilities are vast, spanning 84 offerings in nine product groups. DXC's product groups include Analytics and Engineering, Applications, Business Process Services, Cloud and Security, Modern Workplace, and IT Outsourcing. DXC's security proposition leverages the company's long history in large-scale complex integration, managed services, and enterprise application lifecycle management for large-scale systems.

DXC has a significant global market presence, of which 50% of revenues come from the Americas, 30% from Europe, 14% APAC, and 6% from Africa. DXC employs approximately 3,000 security advisors and operates nine Security Operations Centers on five continents.

Universe Assessment

DXC's strengths include strong peer recommendation, a degree of service flexibility in security, complemented by a broad wrapper of IT services capabilities around security and an extensive security roadmap.

DXC has strong peer recommendation. In advocacy, DXC achieved a peer recommendation score of +47, ranking third overall among Universe providers. Surveyed customers ranked their experience with DXC's threat intelligence, as well as the provider's cybersecurity service capability and breadth, very highly.

Advisory led and tailored services to meet client's business drivers. DXC offers a high degree of breadth, scale, and service flexibility across customers' complex IT estates. Such breadth could be confusing to Enterprise buyers. The "Enterprise Technology Stack" is a DXC conceptual framework to help customers with IT modernization, including on-premises and cloud, data-driven operations, and workplace modernization. It includes embedded security capabilities within a broad set of service and sector-specific offerings.

DXC's advisory services seek to embed the company's integrated security services within an organization's enterprise IT architecture. DXC can incorporate its own scalable cyber defense security platform (SIEM/SOC) combined with third-party partner capabilities. Combining with the Enterprise IT stack, DXC's systems integration, outsourcing, and industry specific expertise and is a strength in security services.

Innovation led security services. A good example of how DXC implements solutions is through its "innovation squads," enabled by a "Cyber Reference Architecture" (CRA).

DXC's "innovation squads" employ agile methods to understand a client's business drivers before matching them with DXC's integrated security solutions capabilities. DXC innovation squads bring mature ideation capabilities combining industry and technology expertise that assess requirements across encryption, verification, monitoring, and securing a company's complex IT environments, doing so within a client's industry and legislative contexts and their client's risk appetite.

DXC's "Cyber Reference Architecture" aligns DXC's comprehensive pre-built solutions within a client context. The CRA comprises a set of security blueprints from the strategy layer (e.g., strategy, leadership and governance, and governance risk and compliance), intelligence, and operations layer (e.g., DXC's Cyber Defense and Security Orchestration, including threat intelligence and SIEM/SOC) through to the controls layer (e.g., Identity & Access Management, Application Security, and Physical Security). DXC's CRA model has a degree of service flexibility to meet clients at their level of need, from baseline security (e.g., core network NIDS/NIPS, CASB, DDoS) to more sophisticated threat protection and managed security services.

Strong industry expertise in security. DXC also has substantial industry experience in securing complex environments. Example offers include DXC's Healthcare Cloud and Securing IoT in

Manufacturing. Sample case studies include application security services at a large US critical services provider and deploying a malware detection solution at Italy's National Institute for Insurance Against Accidents at Work (INAIL).

Comprehensive security roadmap. DXC presents a comprehensive strategic roadmap for security innovation that reaches its 2024 vision of "orchestrated predictive security analytics and response from anywhere." Its planned investments in security span all portfolios and correspond with emerging challenges (e.g., 5G and OT security, digital identity across the hybrid cloud, cloud security compliance and data protection, business intelligence integrated risk, and compliance management). Moreover, to DXC's credit, the company articulates its service portfolio particularly well. Many service providers focus on individual security technologies and platforms, to the detriment of net business outcomes.

DXC's opportunities and threats include addressing the role of network transformation, more specialized security providers, and bringing clients along with DXC's security roadmap.

Addressing network led transformation security. It is difficult to fault DXC's breadth of capability, including network security. But customers with an elevated focus on network-based, instead of application-based, organizational transformation may lean towards other service providers. For example, some providers emphasize tight integration interdependencies between the underlying network transport layer, edge, and shift to hybrid cloud. DXC does have clear plans in hybrid cloud management across infrastructure, identity, and platforms to deliver integrated security across the IT stack.

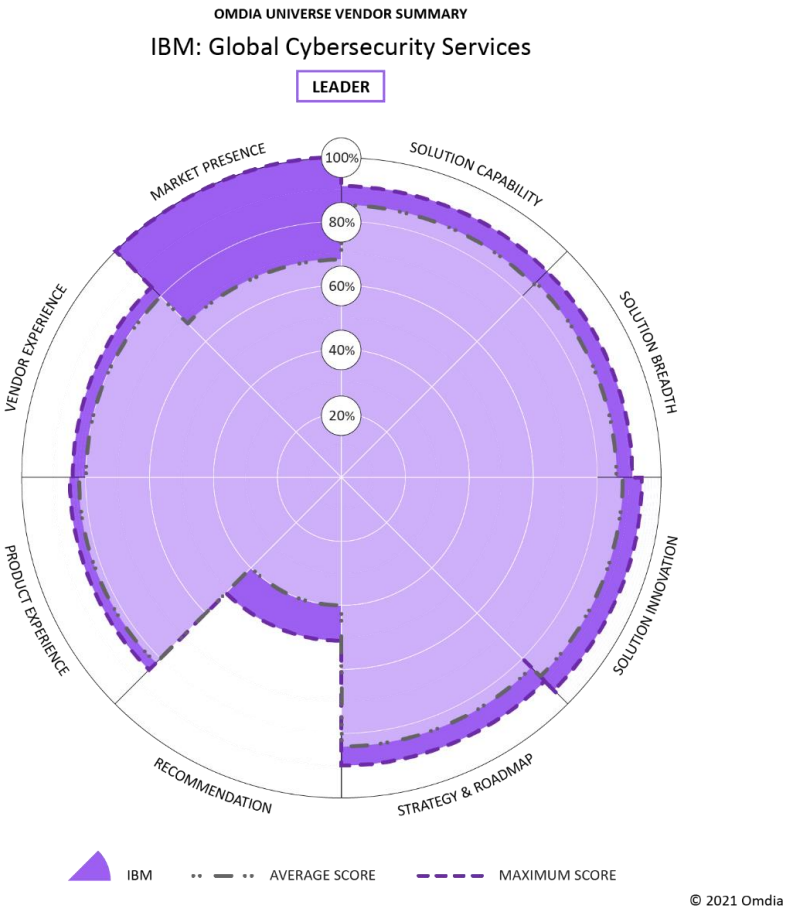
Lifting customer perception. DXC fared less well regarding customer perceptions around vendor experience in security, especially industry security services. Customers also did not necessarily feel clear on DXC's cybersecurity strategy & roadmap. These criteria were ranked relatively low compared with other providers**.** DXC's comprehensive roadmap, industry experience in large scale outsourcing and transformation, and the practical frameworks including its CRA areas are a solid place to address this perception gap.

IBM (Omdia recommendation: Leader)

IBM should appear on shortlists for enterprises that value tightly integrated security services, excellence in expertise and global reach, an ability to execute at scale, open platforms, and industry peer recommendations.

IBM is the market leader in this IT security services Universe. The company has substantial IT security revenues, extensive global presence, well-knit integrated security breadth, and service capability, and continues to innovate in line with a clear roadmap. IBM achieved the highest Peer recommendation score of all providers, and customers rated IBM very high across all vendor experience and product experience categories.

Figure 7: Omdia Universe ratings: IBM



Source: Omdia

Service Provider Summary

IBM Security is a business unit within IBM's Cloud & Cognitive software division, the fastest growing division within IBM globally in 2019, and a vital strategic pillar to IBM's future growth. In October 2020 IBM announced plans to execute a tax-free spin-off of the Managed Infrastructure Services business from its Global Technology Services segment ("NewCo") by the end of 2021. The purpose of this spinoff is to achieve growth in what IBM estimates is a $1 trillion hybrid cloud market, leveraging its open hybrid cloud and AI solutions, enabled by its acquired Red Hat OpenShift platform. IBM Security's software, consulting and managed security services will remain with IBM after the spin-off and the two companies will continue to partner in providing security software and services to their mutual clients.

IBM is among the largest service providers in this Universe, with $77bn in total revenue (2019) and approximately $2.5bn derived specifically from security products and services. The Americas represent approximately 47% of IBM's total revenue, EMEA 32%, and APAC 21%.

IBM customers span 95% of the Fortune Global 500 and the business is supported by approximately 10,000 employees, making it one of the largest security enterprise security providers in the market. IBM delivers services through 12 primary operations centers, with seven global and five regional SOCs, and leverages dozens of "sub-processors" (IBM subsidiaries and third parties) to deliver more localized managed security services.

Universe Assessment

IBM's security strengths are high customer recommendation, global presence, security portfolio breadth, depth, industry credibility, and continuing innovation.

IBM leads peer recommendation. In overall recommendation/advocacy of the global surveyed customers, IBM achieved +51 Peer recommendation score, ranking first. IBM also ranked first in most Vendor Experience and Product Experience categories.

Significant market presence. IBM has large security revenue, broad reach across locations, and the highest overall share of wallet in security services. Omdia's security survey found that 73% of respondent large enterprises worldwide have an existing relationship with IBM, nearly double that of any other security provider (Accenture and AT&T had 38% of customers with an existing relationship).

Broad and integrated security services. IBM comes from a heritage in large-scale consulting, systems integration, and outsourcing that led to its market-leading service capability in security. IBM's breadth combines proprietary, open-source, and third-party capabilities, most notably in the QRadar and Resilient security solutions.

IBM's QRadar Product Family offers Security Information, and Event Management (SIEM). The platform is available on-premises, in the cloud, and with AI augmentation through Watson. Built-in analytics can detect threats, and pre-integration capability exists with 450 solutions, including extensive third-party solutions.

The company's Resilient security is a security orchestration, automation, and response (SOAR) platform combined with IP (AI + ML). Upon approval, IBM can take automatic remediation actions on the client's behalf. The AI algorithm is IBM's Advanced Threat Disposition Scoring (ATDS) that can separate true from false positives, fed by internal threat research from the company's X-Force Exchange and X-Force Incident Response and Intelligence Services (IRIS) team along with external threat intel.

Flexible delivery options, despite size. IBM supports delivery models spanning on-premise, multi-tenant cloud, dedicated deployment in the provider data center, and on-premises take-over of existing technology. Its preferred delivery model is a hybrid delivery model of near-shore on-site personnel and 24x7 remote monitoring and remediation from regional SOCs. For businesses with data sovereignty requirements, this model keeps client data within the region.

Funding further physical expansion. IBM plans to invest in its global SOC expansion. The company has opened a Middle East based SOC in Saudi Arabia, Cyber Range (mobile command/demonstration center) in Bangalore, India, and will promote its SOC in Sydney, Australia.

Expanding cloud security. In hybrid and multi-cloud security, IBM is innovating through integration, doubling down on cloud through productized IBM Cloud Paks that leverage its Red Hat acquisition. IBM Cloud Pak for Security is containerized software pre-integrated with Red Hat OpenShift. IBM Cloud Pak for Security connects to existing security tools using open standards. The platform can search for threat indicators across hybrid, multi-cloud environments, and connects workflows across the business using a unified interface.

Leading industry expertise. IBM drives industry expertise by aligning IBM sellers, associate partners, senior consultants, and architects with industry verticals. The company works with clients to align/apply IBM's security services to industry-specific use cases, including meeting local regulatory and compliance mandates. These industry requirements tend to be strongest in financial services, distribution, and retail, industrial and manufacturing, healthcare and public sector, energy and utilities, and communications industries.

Continued innovation. The company's industry innovation includes the recent launch of a new Threat Intelligence Sharing Platform as part of a private-public partnership for cyber defense serving local and state governments and businesses. IBM also has released X-Force Threat Management for IoT, operational technology (OT), and Internet of Medical Things (IoMT), that allows organizations to discover, profile, and monitor devices in these vertical environments.

IBM's opportunities and threats include emerging and niche service providers with growing end to end capabilities and strong local relationships, and elevating threat intelligence differentiation.

Competing with capable niche providers. As with other large systems integrators and outsourcers, IBM's breadth of capability does include network security. However, customers with an elevated focus on network-based organizational transformation instead of application-based IT transformation may lean towards telco service providers. Further, regional, and global enterprises outside the Fortune 500 may lean more towards smaller security providers within their domestic market with strong local relationships. These companies may look to providers investing heavily in end-to-end capabilities such as BT, or pure-play service providers in security such as Secureworks.

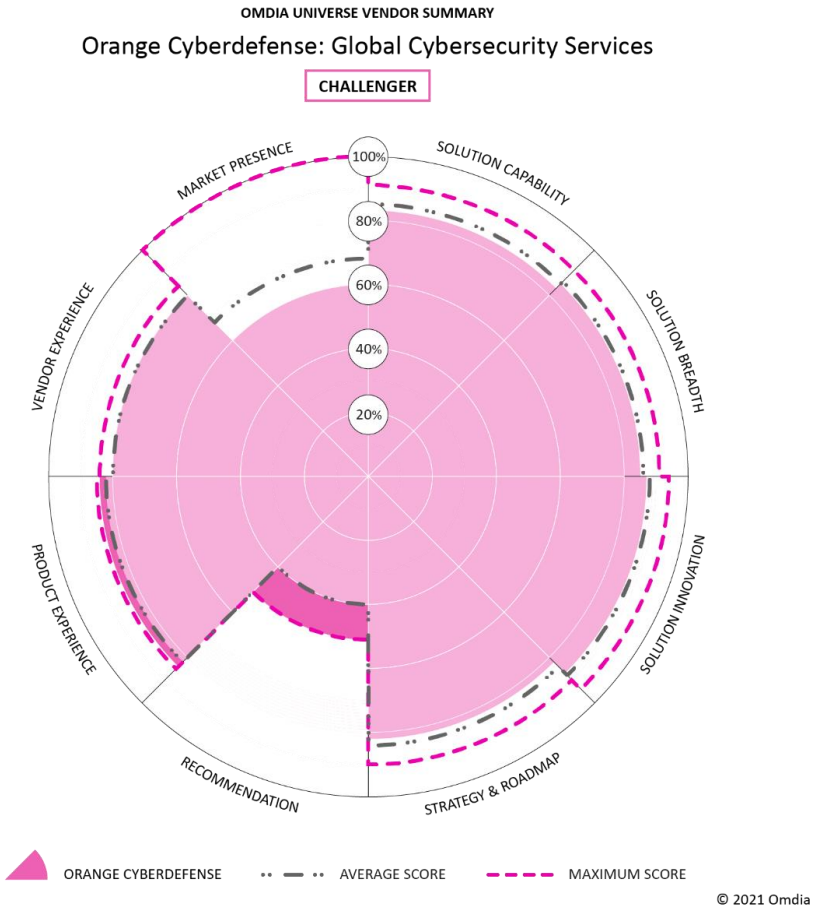
Improving perception of threat intelligence capability. IBM customers scored the company well in all categories except threat intelligence. Omdia suggests that IBM may raise its profile in threat intelligence with existing customers in a competitive and rapidly evolving market, possibly by showing off cloud integration and IBM's AI/ML expertise. Omdia notes some of IBM's competitors are making significant investments to build out end to end capability around Threat Detection and Response and are ramping up the volume and/or sophistication of their threat intelligence feeds.

Orange Cyberdefense (Omdia recommendation: Challenger)

Orange should appear on enterprise shortlists because of its market-leading European presence, IoT experience, and growing focus on the cloud.

Omdia views Orange Cyberdefense as a strong challenger in global IT security services. The provider offers comprehensive security services and demonstrates industry security innovation, especially in the IoT and OT. Orange also scored second overall in peer recommendation score and third in product experience.

Figure 8: Omdia Universe ratings: Orange Cyberdefense



Source: Omdia

Service Provider Summary

Orange Cyberdefense is the Orange group's cybersecurity business arm, established as a standalone business in 2018 to support enterprise demand and faster company growth. The unit brings together acquisitions of Atheos (2014), Lexsi (2016), and Securedata and Securelink (2019).

The provider’s security services have grown from a strong European into a broad global presence. Supporting 4,000 international security customers through 17 SOC's.

Universe Assessment

Orange's strengths include relatively high customer recommendation, a substantial European presence expanding globally, service innovation in co-creation and centers of excellence, and maturing Managed Detection & Response capabilities.

Market leading customer recommendation. In overall recommendation/advocacy of the global surveyed customers, Orange Cyberdefense achieved a peer recommendation score of +51, on par with the market leader IBM (albeit with a smaller customer base).

Orange customers scored the company comparatively well in vendor experience, especially security services breadth and security strategy and roadmap. In product experience, customers also rated Orange well in security specific “consulting and integration,” “industry solutions,” and “technology services” customer satisfaction ratings.

Growing market presence outside Europe. In terms of market presence, Orange Cyberdefense is a European centric integrated security provider. However, Orange’s capabilities are global and compete with global security service providers.

Worldwide capabilities include 11 CyberSOCs providing threat analysis, detection, and response (Located in UK, France, Sweden, China, Russia, Germany, Poland, Netherlands, and India). 17 SOCs providing technology management and monitoring (located in the US, Norway, Belgium, Mauritius, Malaysia, and CyberSOC locations). And 4 CERTs delivering cybersurveillance and incident response (located in Canada, Singapore, and France). Orange Cyberdefense is also one of the only global players with direct CyberSOC presence in China and Russia, able to comply with local security laws.

Security service flexibility. Orange’s go to market model is intelligence-led and offers some degree of service flexibility across its products, resulting in more customized (but not necessarily bespoke) services to suit different customer needs. For example, Orange offers pre-built integrated security services that finds a balance between bespoke and generic, aligned to client's business, threat context, desired risk profile, budget, and use cases.

Security co-creation and centers of excellence. Orange has invested heavily in co-creation capabilities and innovation labs. Such capabilities give the company an enviable position in services that secure IIoT systems. Orange partners with industrial technology service providers (e.g., Siemens) and customers (e.g., establishing the Industrial Security Alliance with customers such as Total, Air Liquide, Naval Group). Innovation emerging from these alliances seeks to address IT/OT/ICS integrated security in industry verticals such as Transport (e.g., IoT security for rail transmitters for a rail company), manufacturing (e.g., development of OT honeypots co-developed with Orange R&D and industrial alliance partners) and healthcare.

Orange has also invested in centers of excellence across several managed security services, e.g., MDR, Ethical Hacking (including penetration testing), Threat Intelligence (including vulnerability intelligence and assessments), Identity and Access Management, and Security Infrastructure (including managed IDS/IPS, firewalls, web gateway) and OT security. These centers of excellence include participants from Orange Cyberdefense, the Orange Group ecosystem (including R&D, Orange Digital ventures), partners, start-ups, and customers.

Evolving managed threat detection and response. The Orange (MTDR) service capability is rapidly maturing. It includes integrating threat detection across endpoint, logs, networks, OT/ICS, open/deep/dark web, managed services, and proactive threat response, including isolation and takedown services. Orange offers its MTDR service in six variations and fed by 500+ public and proprietary intelligence services, leveraging ML/AI (e.g., automated malware analysis), big data, and SOAR for internal service assurance. Three hundred cloud security specialists globally support the MDR platform (running on Splunk), integrating through APIs to major cloud platforms: GCP, AWS, and Azure.

Positive customer references. Orange supplied two European customers customer references for this Universe assessment. One is a large European engineering consultancy company, the other is one of the world's largest cooperative financial institutions. Both companies were complimentary of the provider's capability and experience across Managed Vulnerability, Managed Detection, and Response (log/SIEM based), penetration testing, plus integration of Endpoint Protection, Email Protection, and Secure Access Management. Further, they noted Orange's ability to bring service customization with its security offerings, although this came with some onboarding effort.

Opportunities and threats to Orange include depth of capability and brand awareness outside Europe, broader vertical experience outside OT/IIoT specific use cases, and threat intelligence capability perception.

Increasing brand awareness. Orange Cyberdefense was established in 2016, spun out of Orange Business Services into a dedicated Business Unit of the Orange Group in 2018.

The company should continue to develop a unique cybersecurity identity, as Orange is still less well known outside Europe. Lack of brand awareness is a challenge in a crowded market where threat intelligence and technical excellence are not enough to automatically make it onto MNC shortlists: The brand fights for awareness and consideration, and against existing security partner preferences. While international, Orange Cyberdefense is not at the same level of scale and reach in all parts of the globe. However, its business is growing in the US. Growing presence across more geographies in their footprint will boost its service capability.

Expanding repeatable industry security presence and offerings. Orange's strategy and roadmap includes investment in OT/IIoT security vertical use cases. This innovation model is not easy and requires an ongoing commitment to partnership and funding. The company can differentiate itself through continued investment to ramp up services offered for manufacturing, utilities, energy, and transportation customers specifically related to Operational Technology (OT) and Industrial Internet of Things (IIoT) security. Orange Cyberdefense will be able to leverage this expertise into adjacent industries (e.g., professional services complement expertise in government and communications sectors.) Integration between Orange Cyberdefense and Orange Business Services offerings can

leverage the telco services, but also give enterprises the option to remain service provider neutral and security focused.

Increasing perceptions of threat intelligence capability. Orange scored relatively lower than Universe peers in product experience for threat intelligence and vendor experience on the degree of security innovation. These are two areas for Orange Cyberdefense to address. Especially given the company's focus on MTDR (including embedded threat intelligence), IoT/OT investments and high overall recommendation scores.

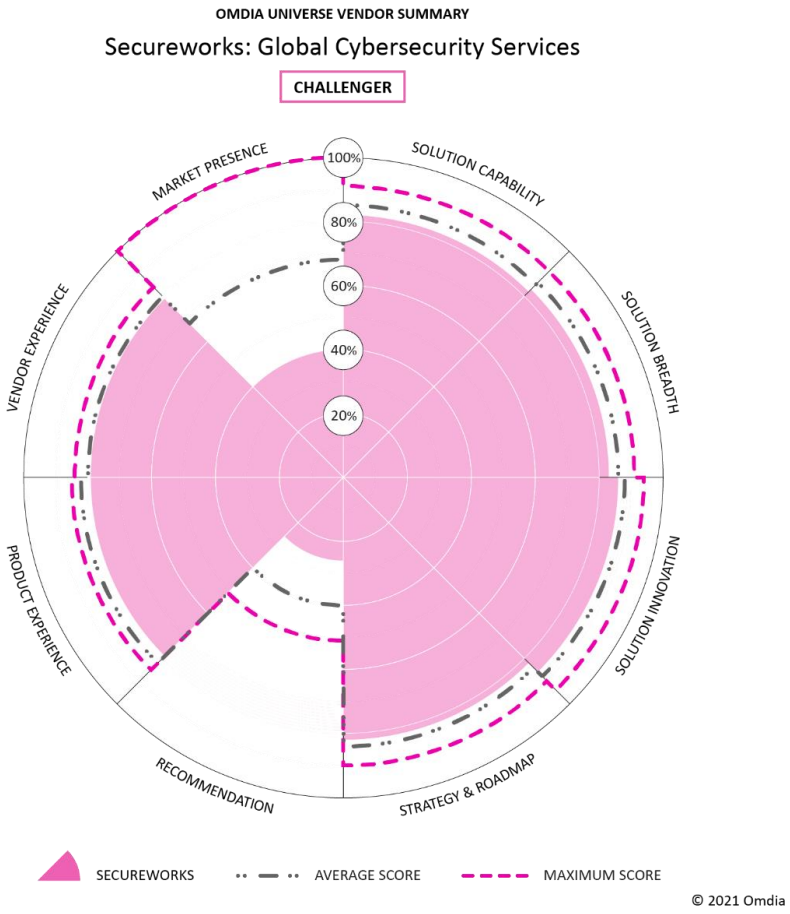
Secureworks (Omdia recommendation: Challenger)

Secureworks should appear on shortlists for enterprises that value a dedicated, specialized security provider with a strong platform focus.

Secureworks is a focused challenger in global IT security services. An established vendor and the only company in the Universe that is exclusively focused on security, Secureworks differentiates itself through a concentrated IT security focus across managed services, incident response, security consulting, and professional services underpinned by its Taegis™ XDR platform.

Customer satisfaction scores were highest for the provider's Threat Intelligence product experience and perceived vendor experience in security.

Figure 9: Omdia Universe ratings: Secureworks



Source: Omdia

Service Provider Summary

Secureworks is the only specialized, pure-play provider of IT Security services supporting more than 4,000 customers in over 50 countries. Established in 1999, its revenue to the fiscal year ending January 31, 2020, increased 6.6% to $552.8m. Founded in 1999 Secureworks has an established presence in North America, Europe, and APAC.

Since 2019, Secureworks' go to market strategy has become increasingly channel-focused, through a Global Partner Program of channel/resellers/alliance partners. Secureworks also recently added a new world-wide Managed Security Service Provider (MSSP) initiative to expand reach. Partners have access to Secureworks' extensive telemetry, analytics, and expertise through Taegis™.

Universe Assessment

Secureworks' strengths include its exclusive security focus, SaaS provisioned Taegis XDR/VDR platform backed by its deep analytics, and an indirect channel growth strategy.

A dedicated security services provider. A significant point of differentiation from other Service Providers in this Universe is Secureworks' exclusive and in-depth focus on Cybersecurity as a standalone provider. Other service providers offer security that are often within or attached to telecommunications and networks, outsourcing, or system integration/consulting services. Secureworks has built a level of expertise from 20 years of exclusive focus on security, which it labels as its "network effect." Secureworks claims continuous learning and improvement from decades of detecting and responding to advanced threats.

Product advancements in threat detection and response. IT security is becoming more complex and adversaries are becoming more sophisticated. Secureworks continues to invest heavily in AI/ML-driven analytics, software, and people, using extensive data sets through its Taegis Extended Detection and Response (XDR) platform and Secureworks Taegis Vulnerability Detection and Response (VDR) analytics.

Taegis is SaaS-enabled, providing analytics, machine learning, and deep learning strategies, collectively called "detectors," to identify suspicious and malicious activity. The platform provides turnkey analytics, applied intelligence from the (Secureworks Counter Threat Unit research team), set pricing, EDR capabilities including cloud environment support, and is also mapped to US research organization MITRE's ATT&CK Framework to provide a common industry terminology for communicating techniques and tactics.

Secureworks offers customers including other MSSP's access to security services via this proprietary XDR platform, carefully decoupling aspects of its services and platform components. The provider also offers managed service wrappers and consulting for organizations via services.

Accelerating global reach and scale through partners. Secureworks runs a Global Partner Program of channel/reseller/alliance partners, which includes access to Taegis. Secureworks has a high degree of focus and investment in making its indirect business model a success, at the possible loss of concentration on the direct channel.

Omdia believes this channel and product approach has the strongest appeal with three customer sets. Firstly, large enterprises with in-house IT Security that want access to cost-effective security coverage for mission-critical applications and have a moderate security infrastructure. Second, industry-leading companies that desire to improve their capabilities with a broad and complex security environment. Third, channel partners that enable these use cases and drive reach within regions or industries.

Further, this channel and platform approach will strengthen Secureworks' position in the emerging lucrative multi-cloud security management services market, enabling firms to digitally transform while contending with more advanced threats, skills shortages, and a crowded service provider marketplace.

Opportunities and threats to Secureworks include maintaining intimate customer relationships across the channel and the degree of depth and focus on industry-specific security challenges.

In advocacy, Secureworks needs to lift its level of recommendation. In the overall peer recommendation of the global surveyed customers, Secureworks scored +26. This is a positive score, but lower than Universe peers, ranking seventh overall.

Based on customer product experience rating, Secureworks should focus on customer perceptions of their managed security services and Security Technology Services as a priority. The lower relative scores in these areas suggest a disconnect between the provider's experience, its NG-SIEM platform, and channel model relative to its target customers' journey. For example, co-innovation, labs, and thought leadership are a big focus for other managed security providers, and this, alongside the continued quality of experience, should be a focus for Secureworks as it expands the use of channel partners.

Omdia notes the recommendation survey was issued prior to the Taegis platform release, which is expected to quickly improve customer perceptions in this area.

Targeted indirect channel model for coverage and capability. Secureworks' indirect channel model is a sizeable growth opportunity, and Secureworks' shift in approach to the next generation SOC should be attractive to channel partners globally. A challenge will be large enterprises that need cross-region support, have complex IT and digital transformation to address, and want to outsource end to end security.

Addressing industry specific needs. Secureworks could explore higher degrees of industry-specific services, developed directly or through partners, in its target industries. The provider has decades of security-focused experience services, a scalable TDR platform, and established customers across manufacturing, financial services, retail, business and professional services, healthcare, energy/utilities, and others that offer additional growth potential.

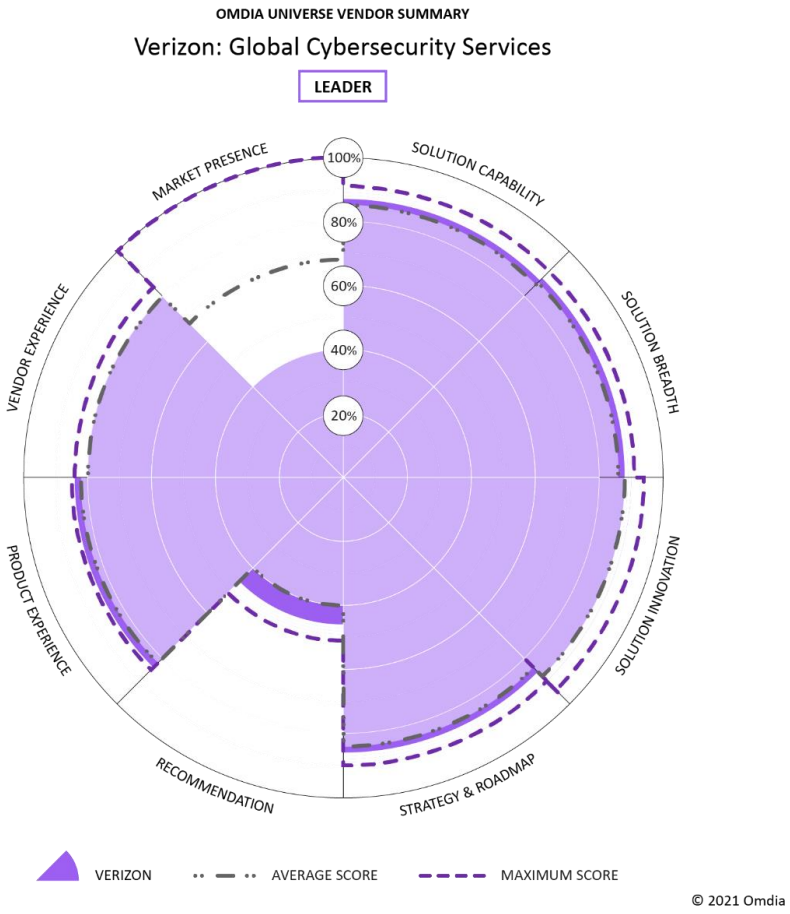
Verizon (Omdia recommendation: Leader)

Verizon should appear on shortlists for enterprises that want a global telco with broad security capabilities, 5G and cloud security innovation, strong client references, and overall peer recommendation in security.

Verizon is a market leader in this managed IT security services Universe. Verizon is smaller than other providers and its primary business is networks, but the company punches above its weight in security. The provider offers considerable depth and breadth of IT security expertise, global presence, industry expertise and it is the only telco to achieve a Leadership title.

Verizon rated an impressive third in overall peer recommendation scores and achieved high satisfaction ratings in consulting & integration, threat intelligence, and technology services.

Figure 10: Omdia Universe ratings: Verizon



Source: Omdia

Service Provider Summary

Verizon security services reside within the Verizon Business Group and are among the principal services offered to enterprise and public sector customers. Verizon Business provides wireless and wireline communications services and products, video and data services, corporate networking services, security and managed network services, voice services and network access. Verizon Business Group's global scale enables Verizon's security services reach. Verizon is headquartered in the US, operating globally, including EMEA and APAC.

Verizon security services revenue has recently grown at double the market rate, with ~3,500 customers globally and supporting 97% of Fortune 500 companies. 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. Also of note is Verizon's Data Breach Investigations Report and other prominent security thought leadership.

Universe Assessment

Verizon's strengths include strong peer recommendation, broad security capability, a roadmap for clients' network-based digital transformation, security thought leadership, and maturing managed detection and response.

A leader in peer recommendation. In the overall recommendation/advocacy of the global surveyed customers, Verizon achieved +46, the third-highest overall rating amongst service providers. Customers rated Verizon's security service experience highly in consulting and integration, threat intelligence, and technology services.

Excellent breadth of security services, despite a smaller size. While not the largest service provider by security revenue, Verizon punches above its weight, offering a broad portfolio of security services globally, complemented by an ecosystem of channel partners. Verizon has excellent breadth across security professional and managed services. These capabilities seek to enhance cyber risk visibility, manage impact, and restore operations, detect and respond to attacks faster, and reduce an organization's attack surface.

Strong story in network led transformation. As a leading global telco, Verizon also has a strong core competency in IoT, 5G, and network security from running wireless, software-defined enterprise networks on behalf of customers globally.

Verizon is well-positioned for growth around network and digital transformation with compelling roadmaps that address the security and industry challenges of emerging technologies such as blockchain, IoT, quantum computing, machine learning, and artificial intelligence. Examples include:

- 5G labs as a testing ground for new security use cases in collaboration with industry partners, academia, start-ups, and labs (e.g., Google X Labs, MIT Cyber Lab).
- A cloud-native operating model to improve end to end customer provisioning of multiple products (e.g., ATLAS Platform for integrated Security Services).
- Verizon Identity blockchain-based identity proofing service; and
- SIM Secure, binding physical phone to SIM card using blockchain security.

Recognized as a security thought leader. Verizon has achieved standout thought leadership and offers clients deep cyber-security insight and knowledge as both a producer and a consumer of cyber threat intelligence. Verizon owns and manages over 800,000 route miles of network cabling worldwide, and over 60% of the world's internet traffic touches its network at some point. The provider leverages these intelligence feeds, producing indicators of compromise (IOC) as part of its defensive strategy on its global network. The company also has research partnerships with universities, cooperative research, and development agreements (CRADAs) with government agencies and participates in the Vocabulary for Event Recording & Incident Sharing (VERIS) community.

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

Evolving managed detection and response. Verizon continues to invest in managed detection and response services to integrate threat intelligence, SOC services, incident response, research, and experience from managing its global network in terms of innovation. The MDR cloud-based service leverages analytics and behavior modeling to identify potential cyber threats. The service also overlays Verizon's core remote threat monitoring, detection, and response capabilities with built-in multi-layer analytics and behavior modeling from Securonix.

Strong marquee client references. Verizon also provided a high-profile APAC public sector client reference. The client commended Verizon's ability and willingness to be flexible and commit to stringent SLAs for critical infrastructure services. The reference client described choosing Verizon not on price but on its security expertise and was very likely to recommend the company to peers.

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. Verizon faces increasing competition from other telcos in this Universe, which are rapidly expanding their security capabilities. Some telco competitors also leverage their US market presence. Others are cybersecurity leaders developing breadth across regions and depth with SOC investments, skills, and integrated platforms. Service providers with strong customer relationships, a clear roadmap, and industry expertise in specific areas challenge Verizon's thought leadership.

Additionally, Verizon will come up against global integrators and managed services providers with deep client relationships in large enterprise and government client segments. These providers offer extensive industry-specific security expertise, in-depth consulting, and integration experience, factors that challenge large enterprises as they rapidly digitize. An opportunity for Verizon is to lead security around digital transformation enabled by IoT and 5G. "Industry 4.0" will change entire business models requiring deep business and technology experience extending beyond the network.

Increasing customer awareness. Surveyed customers ranked Verizon slightly lower compared to other Universe providers, namely in degree of security service breadth and understanding of the provider's security strategy and roadmap. While this did not appear to impact the overall recommendation rating, Verizon should address possible perception gaps by showcasing existing references, capabilities, and anchoring these to their established industry thought leadership.

Methodology

Omdia Universe

Omdia invited select providers with evident market presence and capability breadth in IT Security globally to participate. Not all providers accepted or were able to respond to both RFI and briefing components. The report drew from these service provider responses, complemented by Omdia peer assessment, reviews, analyst briefings, and additional secondary sources including client-facing websites.

Omdia Ratings

Figure 11 offers a high-level example of the service scoring matrix Omdia used to evaluate qualified service providers. The x-axis represents service provider capabilities holistically, across present and planned capabilities, spanning depth and breadth of current ability in each domain (e.g., security consulting or managed services), degree of market differentiation, level of security innovation, and provider strategy.

Figure 11: Service Capability scoring matrix (managed security scoring table - example)

			---------- Capability Model ----------					
Category	Sub-Category	RFI / Survey Question	1 - Lacks Capability	2 - Minimum Capability	3 - Partial Capability	4 - Broad Capability	5 - Advanced Capability	Evaluated Service Provider Score
Managed Cybersecurity Services								
AA001	Strategy & Roadmap	What is your roadmap for the future? Please outline what additional offerings customer can expect to Managed Cybersecurity services in the	No clear cybersecurity roadmap, M&A or product developments.	Vague, unclear or dated cyber security strategy > 18 months. Some stated product development.	Roadmap published within last 12-18 months, product developments clearly evident (past and future).	Demonstrates examples of 2+ recent/ planned cybersecurity strategy but not as comprehensive or advanced. E.g.	Demonstrated multiple examples of a: MSS is a strategic growth pillar for the vendor; compelling strategy from the perspective of	#
AA002	Innovation	Please outline your innovation approach from the customers perspective across Managed Cybersecurity services, or each of	No referenced or publicly available cybersecurity innovations in past 12-18 months.	One cybersecurity innovation in past 12 months.	2+ cybersecurity innovations in past 12 months	Demonstrates examples of 2+ recent/ planned cybersecurity innovations but not as comprehensive as advanced. E.g.	Demonstrates clear examples of MSS innovations e.g.: Advances in MDR; Patents, Established Centers of Excellence; Integrated	#
AA003	In market differentiation	Who do you consider are your firms biggest competitors in Managed Cybersecurity services? How do your services stand apart from them - how	No referenced competitive differentiators in response or public materials (feature/function capabilities	Limited referenced competitive differentiators in response or public materials (feature/function capabilities	Several referenced competitive differentiators in response or public materials with customer focus.	Multiple, clear referenced competitive differentiators in response or public materials with clear customer focus.	Multiple, clear, compelling customer perspective referenced competitive differentiators in response or public materials.	#
AA004	Breadth of services	Please list your current services and solutions offered across the full breadth of Managed Cybersecurity services. For each, please indicate if it	Apparent gaps in basic managed security services across regions or services. Limited SOC's.	Standalone basic managed security services across major regions or services available.	In region SOC's Standalone basic managed security services across major regions or services available.	Services across all major states MS areas. Available Globally and Regionally. Clearly supported by regional SOC's.	Services across all major stated MS areas. Available Globally and Regionally. Clearly supported by regional SOC's. Offered both as	#
AA005	Depth of services	For each area of Managed Cybersecurity services please indicate the skills, people, processes, tools or other features that demonstrate the	No defining skills, presence, capabilities, customer references or evidence of expertise.	Limited - defining skills, presence, capabilities, customer references or evidence of expertise.	Stated examples or capabilities demonstrating depth globally.	Stated examples or capabilities demonstrating depth globally and regionally. Clear and compelling.	Established scale in number of certified staff and SOC locations. Stated examples or capabilities demonstrating depth globally	#
Overall Managed Security Score								#
Cybersecurity Industry Solutions								
Cybersecurity Consulting and Integration								
Threat Detection and Intelligence								
Cybersecurity Technology Services								
Overall weighted Scores							Total Strategy Score	#
							Total Innovation Score	#
							Solution Breadth Score	#

The y-axis represents the overall Customer Experience Score (CX). Omdia conducted a global primary research survey of 220 senior IT decision-makers at large enterprises across three regions globally. The CX scores used in the Universe survey are based on this primary research. Several service

providers did also provide direct references, which were called upon by Omdia and referenced in respective vendor assessment sections.

The Universe complements the service capability assessment with a view of a customer's experience across various security services they source from providers. Omdia believes this approach represents a complete view of what enterprise clients can expect. Figure 12 offers a summary of sample survey questions and CX ratings.

Omdia commissioned primary research to assess each company's customer experience, across "likelihood to recommend," "vendor experience in security," and "security service experience." Respondents could only assess those providers from which their companies purchased security services (e.g., threat intelligence). Besides using the respondent results for evaluation criteria, the survey also verified that service providers Omdia chose to include in this Universe assessment were partners for a critical mass of randomly sampled large enterprise customers across geographies and industries.

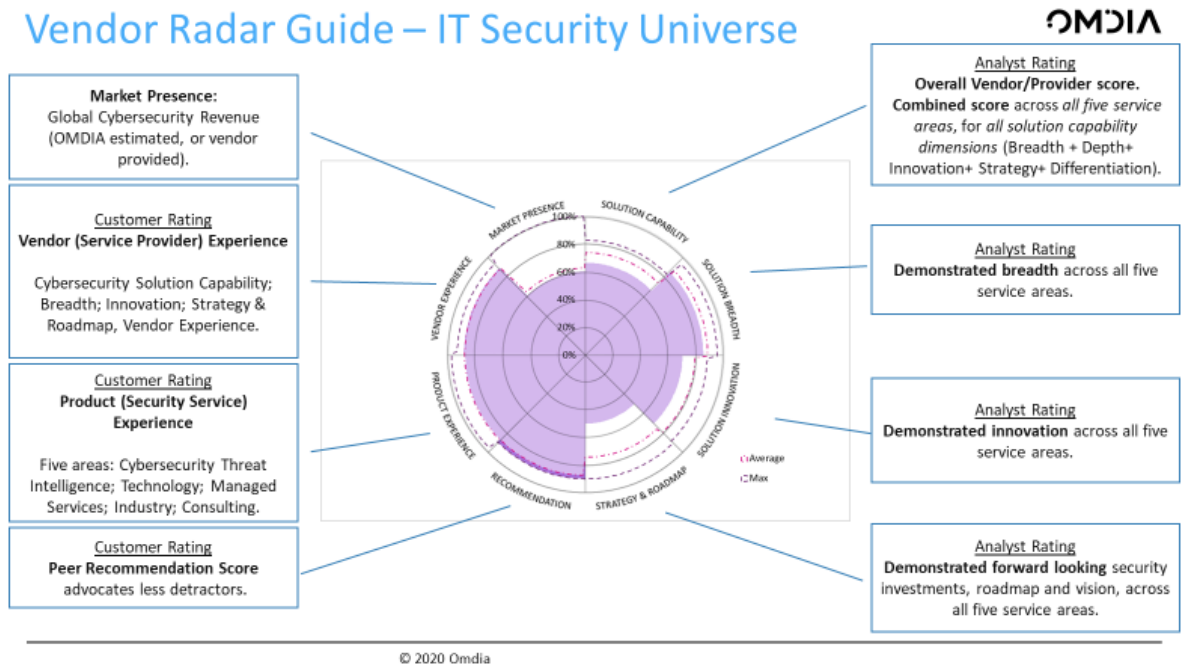
Figure 12: Customer Experience weighting and survey questions

Category	Weighting	Source / Survey Question	Method
Vendor Experience	25%	***How would you rate your security vendor in the following criteria?*** *(Rate each area on a 10-point scale, where 10 = Excellent and 1 = Poor)* Cybersecurity solution capability, The breadth of security solutions, Degree of cybersecurity innovation, Cybersecurity Strategy and roadmap, Vendor experience in security - for chosen/current vendor(s) only.	Overall Service Provider Experience scores across all five categories where: Poor (<4) Average (5-7) Excellent (8-10)
Product (Service) Experience	25%	***What has been the quality of your experience with the partner in the past 12 months?*** *(Rate each area on a 10-point scale, where 10 = Excellent and 1 = Poor* Cybersecurity Threat Intelligence, Cybersecurity Technology Services, Cybersecurity Managed Services, Cybersecurity Industry Solutions, Cybersecurity Consulting and Integration - for chosen/current vendor(s) only.	Overall Service Experience scores across all five categories where: Poor (<4) Average (5-7) Excellent (8-10)
Likelihood to Recommend	50%	***How likely are you to recommend your current security vendor in the following areas?*** *(Rate each area on a 10-point scale, where 10 = Very Likely and 1 = Very Unlikely)* Cybersecurity Threat Intelligence, Cybersecurity Technology Services, Cybersecurity Managed Services, Cybersecurity Industry Solutions, Cybersecurity Consulting and Integration - for chosen/current vendor(s)	Overall customer advocacy (recommendation) scores across all five categories: Poor (<4) Average (5-7) Excellent (8-10)

Vendor Radar

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

Figure 13: Vendor Radar Guide



Inclusion criteria

The criteria for inclusion in the cybersecurity Universe was IT security service providers that:

- Offer IT security services across all five categories: Threat, Technology, Managed Services, Industry Expertise, Consulting, and Integration.
- Operate on a global scale, with a demonstrable depth of capability and market presence both within and across major regions, including APAC, EMEA, and North America.
- Serve at least 500 large enterprise and government customers, with their base spread across all major regions of the world.
- Attribute significant global revenue from IT/cybersecurity services (i.e., more than $500m annually) and have an evident focus on IT security (i.e., standalone or named security division, direct reporting lines for the business unit to the company CEO).

Additional market definition

The purpose of this report includes assisting CIOs, CSOs, and IT decision makers in awareness, consideration, and evaluation of world-leading security service providers against a standard, robust

set of capability and customer experience criteria. Therefore, the terms ICT security, IT security, and cybersecurity are used interchangeably throughout this report. This approach helps focus on comparison of capabilities and customer experience across the five service categories that are most pertinent to global companies. Omdia does, however, recognize some nuances that may assist a more in-depth evaluation of providers at the next stage, for instance:

The service providers in this Universe mainly focus on information security (information-based assets) and cybersecurity (securing access to systems on which the information resides or travels). Other domains closer related to IT security but not the primary focus of these providers include physical and risk. Physical security commonly includes protecting an organization's information through securing physical access, damage, or interference to assets. Risk management often requires a company's CRO to develop, maintain, and implement an organization's end-to-end risk management framework, contributing to the overall governance, risk, and compliance (GRC). Mature security service providers carefully assess an organization's current IT security state against desired goals, in the context of their industry and business priorities, including GRC.

Assumptions

Each provider responded with different degrees of depth and breadth. Of note:

Accenture declined to participate and the Omdia assessment makes best use of publicly available material and analyst assessments.

Omdia revenue estimates are used for Accenture, BT (who provided a briefing only), and DXC.

Many providers were not able to disclose regional revenue splits due to company policy. Where this was the case, global parent company revenues have been used as a proxy.

Additional Service Providers

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

- Alert Logic
- Atos
- Capgemini
- Deloitte
- Fujitsu
- Lumen (formerly CenturyLink)

- NTT
- Infosys
- TCS
- Trustwave
- Wipro

Appendix

Further reading

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

Author

Adam Etherington, Principal Analyst, Digital Enterprise Services.

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