IDC MarketScape

IDC MarketScape: Worldwide Cybersecurity Consulting Services 2024 Vendor Assessment

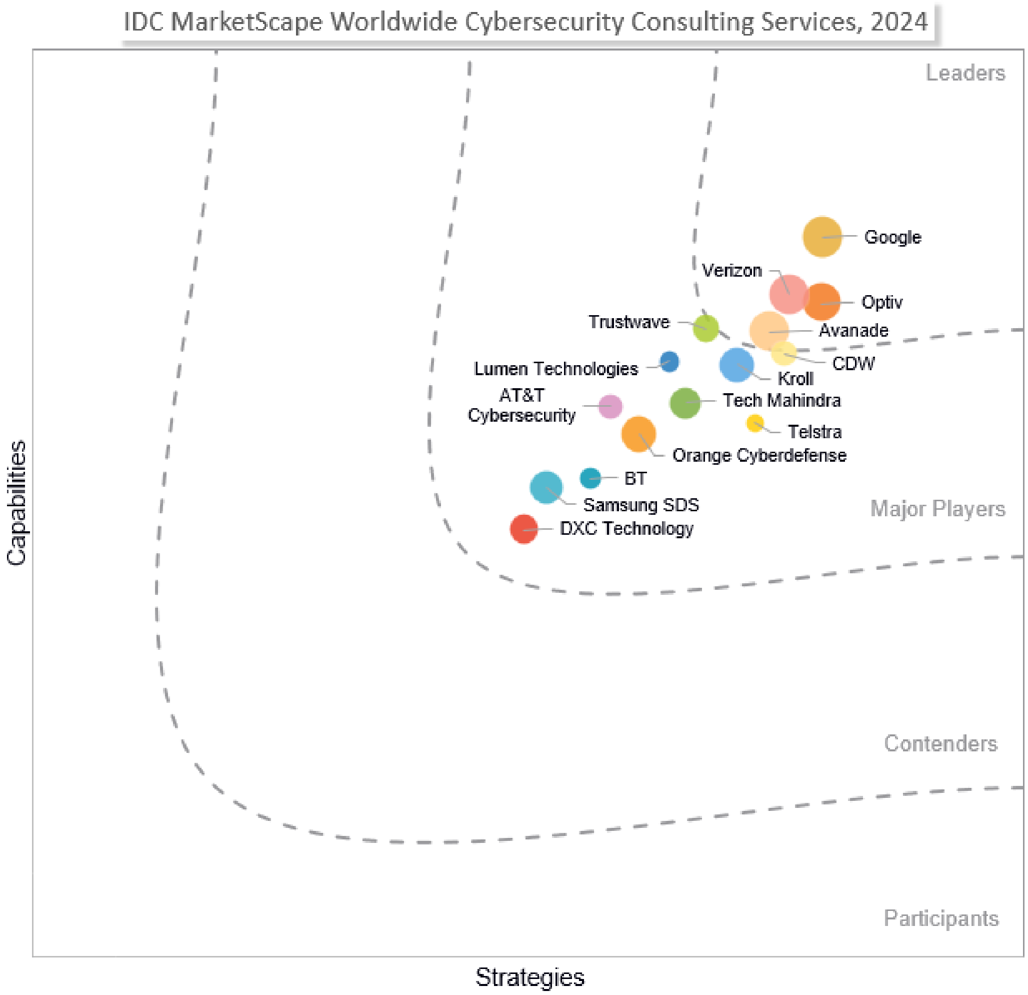
Cathy Huang

THIS MARKETSCAPE EXCERPT FEATURES: TELSTRA

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Cybersecurity Consulting Services Vendor Assessment



Source: IDC, 2024

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Cybersecurity Consulting Services 2024 Vendor Assessment (Doc #US50463223e_Telstra). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Advice for Technology Buyers, Featured Vendor Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

As a growing number of organizations view cybersecurity as a strategic business enabler, along with a surge of regulatory requirements across the world, the quest for quality cybersecurity consultants and trusted cybersecurity advisors hits an all-time high.

In this IDC MarketScape study, IDC assesses the following cybersecurity consulting offerings closely, while most of the featured vendors in this study do have a broader portfolio that goes beyond cybersecurity consulting services:

- Cybersecurity strategy planning and program transformation services
- Security architecture assessment and design services
- Cyber-resilience consulting services

Depending on the requirements, cybersecurity consulting services can be consumed in a discrete, bespoke fashion, but very often services are structured as a component of or integrated into a larger IT or business transformation initiative.

IDC conducted a global survey with 901 organizations to understand the buying trends of cybersecurity consulting services. The survey gathered direct tech buyer feedback for their respective cybersecurity consulting services providers across the world. Most of these firms are featured in *IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment* (IDC #US50463423, January 2024), and the remaining ones are studied in this IDC MarketScape.

IDC finds most of the participating firms have solid technical capabilities and strong cybersecurity skills. Among all the evaluation criteria, "skills and experiences of key personnel engaged in the project" showed positive remarks from the 901 surveyed organizations that utilize the cybersecurity consulting capabilities of the studied firms.

The very nature of cybersecurity consulting services relies heavily on the expertise of consultants. Cybersecurity consultants should have in-depth knowledge and experiences of one or multiple security domains, for example, network security, security operations, incident response, regulatory compliance, and operational technology (OT) security, to support enterprises' needs. Industry-specific knowledge will be a bonus and highly appreciated by tech buyers.

Many of the firms were showing positive output in regard to delivery and people-related criteria, for instance project governance, meeting data privacy and sovereignty requirements, and engaged cybersecurity professionals being very responsive and professional. In contrast, cybersecurity consulting services providers should improve on the innovation aspects, including the proprietary intellectual property (IP), tools, and frameworks used in the engagement and effectiveness of using emerging technologies like AI and generative AI (GenAI) in the delivery and client engagement.

What is more, a good number of security services vendors package their cybersecurity offerings in a highly flexible way. There is a rising trend to package professional security services into a managed-, subscription-, or retainer-based model, such as expertise on demand (EOD) or cyber as a service (CaaS). These models are particularly attractive to midmarket.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in this IDC MarketScape for cybersecurity consulting services, security services vendors must be able to provide services in the categories of cybersecurity strategy planning, transformation, security architecture assessment and design, and cyber-resilience consulting services. Further:

- A security services vendor must operate with a multinational footprint.
- A security services vendor must have a total revenue of cybersecurity consulting services that exceeds $25 million in 2023.

ADVICE FOR TECHNOLOGY BUYERS

In the highly competitive cybersecurity services market, buyers serve their organizations well by expressing assertive expectations and conducting thorough evaluation. Guiding buyers' evaluation, IDC offers the following advice:

- **Multidisciplinary model:** Evaluate vendor's multidisciplinary model and ensure the ability of the vendor to demonstrate an understanding of issues faced by stakeholders including those from outside the security functions such as risk, compliance, operations, IT, networks, finance, and engineering. On this topic, instead of considering an IT tabletop exercise, it might be more useful to have an entire operational tabletop exercise.
- **Addition of training hours:** For a transformation type of project, mandate a certain number of training hours or some cybersecurity awareness sessions in the scope to enhance the overall awareness to the relevant threats, and typical cyberattack techniques. Security breaches often tie back to user actions. Fostering a security-aware culture within the organization is as important as strong security controls. Some of the evaluated cybersecurity services vendors have explicit cybersecurity training or learning and development offerings as part of their portfolio.
- **Innovation:** Innovation demonstrated throughout the engagement is a critical factor to differentiate cybersecurity consulting services vendors. While there is considerable hype around AI, examine the prospect cybersecurity consulting vendors' own way of adopting AI and GenAI, especially how they ensure security and sovereignty issues of AI. Key questions you must ask include:
  - How do you monitor and audit AI systems?
  - What measures do you take to ensure responsible AI practices, including fairness, transparency, and accountability in your algorithms?
  - How are you protecting against authorized data entry into an AI model?

    - How do you plan to bring continuous improvement?
- **Communication:** Consider a vendor's expertise in communicating at the C-suite and board levels. In a cybersecurity consulting project itself, communication and stakeholder management are critical factors of delivering results successfully and on time. In this study, we have assessed vendors' capabilities to support boardroom communication. A handful of vendors do have the capability to articulate risk in the boardroom and effectively connect technical risks to the business challenges without so much technical jargon used.

FEATURED VENDOR PROFILE

This section briefly explains IDC's key observations resulting in Telstra's position in the IDC MarketScape. The description here provides a summary of the vendor's strengths and challenges.

Telstra

Telstra is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide cybersecurity consulting services.

Telstra, a telecommunications company based in Australia, employs approximately 26,000 people. The cybersecurity products and services are delivered by Telstra Security that has 350 cybersecurity professionals, with 150 dedicated to consulting, and an internal Cybersecurity Operations Team of more than 300.

Telstra Security services are delivered by Telstra Purple, the consulting/professional services group within Telstra Enterprise, which together with partners delivers client solutions globally. Consultants are in Australia, Singapore, Hong Kong, the United Kingdom, France, Germany, the Netherlands, and Sweden.

Telstra Security Services deliver security advisory consulting, solutions engineering, and assurance services for cloud and network security, digital identity, and cyberdetection and response. Large organizations typically receive bespoke solutions that can be templated for small and midsize clients. Consultants follow a 4D methodology within a formalized customer delivery framework:

- **Discover:** Focus on future state, establishment of baseline requirements and a prioritized map, assessments, and definition of strategic security objectives such as compliance or risk mitigation
- **Define:** Development of a security strategy and a security target operating model comprising budgets, business case, and transition plan
- **Deliver:** Design, implementation, and handover service to deliver to the target operating model
- **Drive:** Ongoing services such managed security services, monitoring, detection and response services, and cyber-risk quantification services

The underlying principle for Telstra Security services delivery is a consulting-led approach, along with the philosophy – cybersecurity is an enabler for business as well as an apt line of defense against risks and threats. Telstra Security invests in the industry to ensure it is well positioned to provide ongoing support, guidance, and approaches to its customers.

The Security Target Operating Model methodology uses numerous inputs to create a conceptual model (SASE, for example) that can be converted to blueprints and business case options for consulting engagements.

Services align with industry direction and Telstra's strengths to address specific requirements such as compliance and sovereign protection for governments and security for critical infrastructure sectors. To bolster capabilities for security in OT environments, Telstra acquired Alliance Automation and Aqura in 2022. The acquisitions augment Telstra's capabilities in mining and energy-critical infrastructure.

Telstra Security leads with zero trust and NIST global best practices to emphasize visibility and control of security for client organizations and their supply chains. Offerings reflect a combination of proprietary IP and third-party tools and technologies. 6Clicks, for example, is a platform used for cybersecurity advisory and ISMS to demonstrate security maturity level and how to advance it.

Telstra Security has strategic partnership with product vendors such as Palo Alto Networks, Zscaler, Netskope, Cisco, Microsoft and CrowdStrike, Telstra Purple partners, and trusted individuals. Partners may be used in engagements involving client certifications.

The Cybersecurity Operations Team is responsible for threat detection and response for Telstra Security and its clients. The team's scope encompasses SOCs, complex incident response and digital forensics, vulnerability threat strategy and analysis, threat hunting, cyberoperations, and security engineering.

Strengths

- As a carrier, Telstra has a large network infrastructure and data traffic that enable analysis across diverse clients, systems, and endpoints. Real-time visibility aids threat detection, patterns of malicious activity, and potential vulnerabilities.
- The ClubCISO community, which includes 700+ CISOs who can interact with each other through a bespoke application, publishes an annual security maturity report and industry insights.
- The Purple design team brings diverse perspectives to services involving human design. Team members have backgrounds in psychology, game design, academia, design research, visual communications, and interactive design.
- According to client feedback, Telstra's training services along with the cybersecurity consulting work have uplifted the organization's cybersecurity posture and efficacy.
- IDC's *Worldwide Cybersecurity Consulting Services Survey* participants give Telstra a positive rating for the effective use of emerging technologies in its engagement. The provider has also exceeded the peer group average for delivering measurable outcomes and being cost-effective.

Challenges

- The same IDC's *Worldwide Cybersecurity Consulting Services Survey* respondents say Telstra can improve in areas such as the breadth of cybersecurity consulting capabilities, skills, and experience of key project personnel and thought leadership in the cybersecurity space.
- Telstra can also improve its talent retention and management of staff turnover during the project's time to ensure overall service delivery consistency.

Consider Telstra When

Large enterprises, large government departments, and small and midsize organizations of any maturity level that prefer a consulting-led, integrative approach should consider Telstra Security, especially those in Australia, Asia, or Europe. Client challenges may include complex environments, regulations, technology rationalization, and changing company strategies.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

IDC defines cybersecurity consulting services as a range of professional services activities that help organizations plan, design, assess, or transform across their cybersecurity practice. In the scope of this particular IDC MarketScape study, the cybersecurity consulting services include strategy planning and program transformation, architecture assessment and design services, and cyber-resilience consulting. Examples of these services include:

- Security road map development
- Security strategy advisory
- Security operator center (SOC) design and build
- Security sourcing strategy
- Data security and sovereignty advisory
- Identity access management design and transformation

- Integrated threat intelligence design and consult
- Cybersecurity transformation
- Cyber-recovery consulting
- Cyber-supply chain resilience planning
- Architecture assessment services across networks, endpoints, edge, cloud, IoT, OT, and so forth

LEARN MORE

Related Research

- *IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment* (IDC #US50463423, January 2024)
- *What Are the Top Factors Deciding the Selection of Cybersecurity Consulting Services Providers?* (IDC #US51361823, November 2023)
- *Market Analysis Perspective: Worldwide Security Services, 2023 and Beyond* (IDC #US51228723, September 2023)
- *Worldwide and U.S. Comprehensive Security Services Forecast, 2023-2027* (IDC #US50047523, June 2023)
- *IDC's Worldwide Security Services Taxonomy, 2023* (IDC #US50332523, March 2023)

Synopsis

This IDC study represents a vendor assessment of cybersecurity consulting services for enterprises through the IDC MarketScape model. It assesses 15 cybersecurity services vendors offering cybersecurity strategy advisory, architecture assessment and design, cyber-resilience consulting, and cybersecurity transformation services. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for cybersecurity consulting services. The document provides detailed vendor profiles, highlighting their strengths, challenges, and key offerings.

"The role of a trusted cybersecurity partner has increased given the rising importance of cybersecurity to an organization's overall resiliency and success," says Cathy Huang, research director, IDC's Worldwide Security Services. "This trend is manifested in the growing demand for security and risk assessment, security strategy, and program advisory that drives all kinds of vendors, be it telecom providers, managed security pure players, cybersecurity specialists, IT outsourcing providers, or value-added resellers, to put strategic focus to grow their own cybersecurity consulting capabilities."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com